



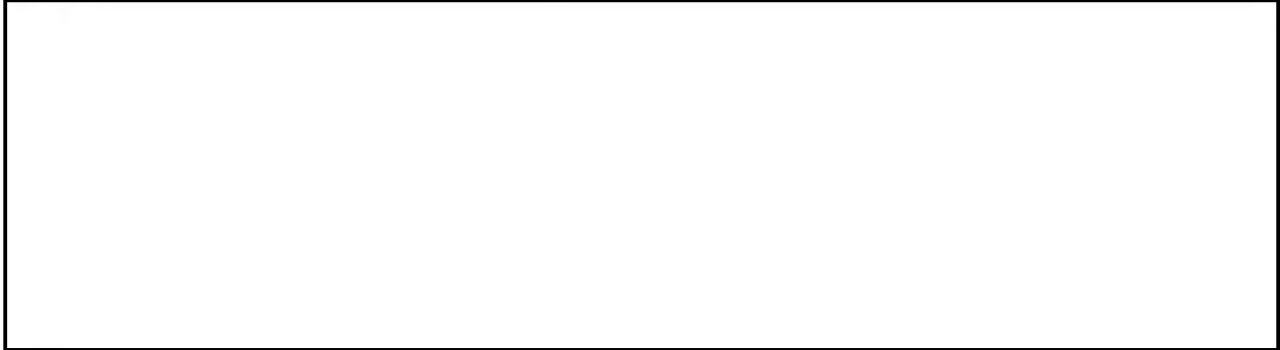
**U.S. Department of Justice**  
**Federal Bureau of Investigation**

July, 2016  
Washington, D.C.

CLINTON E-MAIL INVESTIGATION

MISHANDLING OF CLASSIFIED – UNKNOWN SUBJECT OR COUNTRY (SIM)

(S//NF)

b1  
b3

This report recounts the information collected in this investigation. It is not intended to address potential inconsistencies in, or the validity of, the information related herein.

b3  
b7E

(U//~~FOUO~~) On July 10, 2015, the Federal Bureau of Investigation (FBI) initiated a full investigation based upon a referral received from the US Intelligence Community Inspector General (ICIG), submitted in accordance with Section 811(c) of the Intelligence Authorization Act of 1995 and dated July 6, 2015, regarding the potential unauthorized transmission and storage of classified information on the personal e-mail server of former Secretary of State Hillary Clinton (Clinton).<sup>a</sup> The FBI's investigation focused on determining whether classified information was transmitted or stored on unclassified systems in violation of federal criminal

<sup>a</sup> (U//~~FOUO~~) For a complete listing of the interviews conducted, electronic media collected, legal process issued, and classified e-mails identified during this investigation, please refer to Appendices A-D. As background, Clinton was Secretary of State from January 21, 2009 through February 1, 2013.

statutes and whether classified information was compromised by unauthorized individuals, to include foreign governments or intelligence services, via cyber intrusion or other means. (U//~~FOUO~~) In furtherance of its investigation, the FBI acquired computer equipment and mobile devices, to include equipment associated with two separate e-mail server systems used by Clinton, and forensically reviewed the items to recover relevant evidence. In response to FBI requests for classification determinations in support of this investigation, US Intelligence Community (USIC) agencies determined that 81 e-mail chains,<sup>b,c</sup> which FBI investigation determined were transmitted and stored on Clinton's UNCLASSIFIED personal server systems, contained classified information ranging from the CONFIDENTIAL to TOP SECRET/SPECIAL ACCESS PROGRAM levels at the time they were sent between 2009-2013. USIC agencies determined that 68 of these e-mail chains remain classified. In addition, the classification determination process administered by the US Department of State (State) in connection with Freedom of Information Act (FOIA) litigation identified approximately 2,000 additional e-mails currently classified CONFIDENTIAL and 1 e-mail currently classified SECRET, which FBI investigation determined were transmitted and stored on at least two of Clinton's personal server systems.<sup>d</sup>

(U//~~FOUO~~) The FBI's investigation and forensic analysis did not find evidence confirming that Clinton's e-mail accounts or mobile devices were compromised by cyber means. However, investigative limitations, including the FBI's inability to obtain all mobile devices and various computer components associated with Clinton's personal e-mail systems, prevented the FBI from conclusively determining whether the classified information transmitted and stored on Clinton's personal server systems was compromised via cyber intrusion or other means. The FBI did find that hostile foreign actors successfully gained access to the personal e-mail accounts of individuals with whom Clinton was in regular contact and, in doing so, obtained e-mails sent to or received by Clinton on her personal account.

### 1. (U//~~FOUO~~) Clinton's Personal E-Mail Server Systems

#### *A. (U//~~FOUO~~) Initial E-mail Server: June 2008 – March 2009*

(U//~~FOUO~~) In or around 2007, Justin Cooper, at the time an aide to former President William Jefferson Clinton (President Clinton), purchased an Apple OS X server (Apple Server) for the sole purpose of hosting e-mail services for President Clinton's staff.<sup>1,2</sup> Due to concern over ensuring e-mail reliability and a desire to segregate e-mail for President Clinton's various post-presidency endeavors, President Clinton's aides decided to maintain physical control of the Apple Server in the Clinton residence in Chappaqua, New York (Chappaqua residence).<sup>3,4,5</sup> According to Cooper, in or around June 2008, a representative from Apple installed the Apple

---

<sup>b</sup> (U//~~FOUO~~) The number of classified e-mail chains identified may change as classification determination responses continue to be returned to the FBI.

<sup>c</sup> (U//~~FOUO~~) For the purposes of the FBI's investigation, an "e-mail chain" is defined as a set of e-mail responses having the same initial e-mail. The subject line may be edited in these chains to reflect the purpose of the forward or reply.

<sup>d</sup> (U//~~FOUO~~) State did not provide a determination with respect to the classification of these e-mails at the time they were sent. According to State Under Secretary of Management, Patrick Kennedy, unclassified information provided to State in confidence can later be considered classified when it is "further assessed the disclosure of such information might damage national security or diplomatic relationships." Such information is referred to as "up-class" or "up-classified."

Server<sup>e</sup> in the basement of the Chappaqua residence.<sup>6,7</sup> The FBI was unable to obtain records from Cooper or Apple to verify the installation. At the time, Cooper was the only individual with administrative access to the Apple Server; however, the Clinton family and their Chappaqua residence staff had physical access to the Apple Server.<sup>8,9</sup> The Apple Server initially hosted the domains presidentclinton.com and wjcoffice.com, which were used by President Clinton's staff.<sup>f,10,11</sup>

(U//~~FOUO~~) Prior to January 21, 2009, when she was sworn in as the US Secretary of State, Clinton used a personally-acquired BlackBerry device with service initially from Cingular Wireless and later AT&T Wireless, to access her e-mail accounts.<sup>12,13</sup> Clinton initially used the e-mail addresses hr15@mycingular.blackberry.net and then changed to hr15@att.blackberry.net.<sup>14,15</sup> According to Cooper, in January 2009, Clinton decided to stop using her hr15@att.blackberry.net e-mail address and instead began using a new private domain, clintonemail.com, to host e-mail service on the Apple Server.<sup>16</sup> Clinton stated to the FBI that she directed aides, in or around January 2009, to create the clintonemail.com account, and as a matter of convenience her clintonemail.com account was moved to an e-mail system maintained by President Clinton's aides.<sup>17</sup> While Cooper could not specifically recall registering the domain, Cooper was listed as the point of contact for clintonemail.com when the domain was registered with a domain registration services company, Network Solutions, on January 13, 2009.<sup>18,19</sup> Clinton used her att.blackberry.net e-mail account as her primary e-mail address until approximately mid-to-late January 2009 when she transitioned to her newly created hdr22@clintonemail.com account.<sup>20,21</sup> The FBI did not recover any information indicating that Clinton sent an e-mail from her hr15@att.blackberry.net e-mail after March 18, 2009.

(U//~~FOUO~~) According to Cooper, in or around January 2009 the decision was made to move to another server because the Apple Server was antiquated and users were experiencing problems with e-mail delivery on their BlackBerry devices.<sup>22,23</sup> At the recommendation of Huma Abedin, Clinton's long-time aide and later Deputy Chief of Staff at State, in or around fall 2008, Cooper contacted Bryan Pagliano, who worked on Clinton's 2008 presidential campaign as an information technology specialist, to build the new server system and to assist Cooper with the administration of the new server system.<sup>24,25,26,27</sup> Pagliano was in the process of liquidating the computer equipment from Clinton's presidential campaign when Cooper contacted Pagliano about using some of the campaign's computer equipment to replace the existing Apple Server at Clinton's Chappaqua residence.<sup>28,29</sup> Pagliano was unaware the server would be used by Clinton at the time he was building the server system; rather, he believed the server would be used by President Clinton's staff.<sup>30</sup> Clinton told the FBI that at some point she became aware there was a server in the basement of her Chappaqua residence.<sup>31</sup> However, she was unaware of the transition from the Apple Server managed by Cooper to another server built by Pagliano and therefore, was not involved in the transition decision.<sup>32</sup>

*B. (U//~~FOUO~~) Second E-mail Server: March 2009 – June 2013*

<sup>e</sup> (U//~~FOUO~~) The Apple Server consisted of an Apple Power Macintosh G4 or G5 tower and an HP printer.

<sup>f</sup> (U//~~FOUO~~) Investigation determined various employees of President Clinton maintained e-mail accounts using the presidentclinton.com domain to include [ ]

[ ] President Clinton did not maintain an e-mail account on the Apple Server. The e-mail domain wjcoffice.com was primarily a legacy domain that contained mostly forwarded e-mail.

(U//~~FOUO~~) Between the fall of 2008 and January 2009, Pagliano requisitioned the original hardware for the second e-mail server from Clinton's presidential campaign headquarters in Arlington, VA.<sup>33</sup> In addition to hardware acquired from Clinton's presidential campaign, Pagliano and Cooper<sup>g</sup> purchased additional necessary equipment through commercial vendors.<sup>34,35,36,37</sup> In March 2009, after Pagliano had acquired all of the server equipment and installed the necessary software, he and Cooper met at Clinton's Chappaqua residence to physically install the server and related equipment in a server rack in the Clintons' basement.<sup>h,38,39</sup>

(U//~~FOUO~~) Once the new server system<sup>i</sup> was physically installed and powered on, Pagliano began migrating the e-mail data from the Apple Server to the Pagliano-administered server system (Pagliano Server).<sup>40</sup> Pagliano believed he "popped out" all of the e-mail from the Apple Server and that no e-mail content should have remained on the Apple Server once the migration took place.<sup>41</sup> Pagliano stated to the FBI that he only transferred clintonemail.com e-mail accounts for Abedin and [REDACTED] from the Apple Server and said he was unaware of and did not transfer an e-mail account for Clinton.<sup>i,42</sup> However, Cooper stated to the FBI that he believed Clinton had a clintonemail.com e-mail account on the Apple Server, and that Abedin did not have a clintonemail.com account on the Apple Server.<sup>43</sup> As the FBI was unable to obtain the original Apple Server for a forensic review for reasons explained below, the FBI cannot determine which clintonemail.com e-mail accounts were hosted on, and transferred from, the Apple Server to the Pagliano Server.

b6  
b7C

(U//~~FOUO~~) After the e-mail account migration was completed, Cooper changed the Mail Exchange (MX) records<sup>k</sup> to ensure that delivery of all subsequent e-mail to or from e-mail addresses on the presidentclinton.com and clintonemail.com domains would be directed toward the new Pagliano Server instead of the Apple Server.<sup>44</sup> The Pagliano Server was only used for e-mail management, and the FBI's review of the oldest available backup image of this server, dated June 24, 2013, did not indicate that any e-mail users' files were stored on the Pagliano Server.<sup>45</sup>

(U//~~FOUO~~) In March 2009, following the e-mail migration from the Apple Server to the Pagliano Server, the Apple Server was repurposed to serve as a personal computer for household staff.<sup>46</sup> [REDACTED] at Clinton's Chappaqua residence, subsequently used the Apple Server equipment as a workstation.<sup>47</sup> In 2014, the data on the Apple computer was transferred to an Apple iMac computer, and the hard drive of the old Apple computer, which

b6  
b7C

<sup>g</sup> (U//~~FOUO~~) Cooper had [REDACTED] and was often responsible for reimbursing staff for purchases/expenses.

b6  
b7C

<sup>h</sup> (U//~~FOUO~~) Pagliano visited Clinton's Chappaqua residence on at least three occasions to work on the server: in March 2009, to install the server; in June 2011, to upgrade the equipment; and in January 2012, to fix a hardware issue.

<sup>i</sup> (U//~~FOUO~~) The Pagliano Server initially consisted of the following equipment: a Dell PowerEdge 2900 server running Microsoft Exchange for e-mail hosting and management, a Dell PowerEdge 1950 server running BlackBerry Enterprise Server (BES) for the management of BlackBerry devices, a Seagate external hard drive to store backups of the Dell PowerEdge 2900 server, a Dell switch, a Cisco firewall, and a power supply.

<sup>j</sup> (U//~~FOUO~~) An e-mail obtained during the FBI investigation from Cooper to Clinton, indicated that in April 2009, Cooper was preparing to update Clinton's BlackBerry to "put it on our new system."

<sup>k</sup> (U) An MX record determines which server will handle e-mail delivery for a domain and is necessary for routing e-mail to its proper destination.



previously served as the Apple Server was discarded.<sup>48</sup> On October 14, 2015, Williams & Connolly LLP (Williams & Connolly), counsel for Clinton, confirmed to the Department of Justice (DOJ) that a review of the iMac was conducted, pursuant to a request by DOJ, and no e-mails were found belonging to Clinton from the period of her tenure as Secretary of State.<sup>49</sup>

(U//~~FOUO~~) Pagliano and Cooper both had administrative accounts on the Pagliano Server.<sup>50</sup> At Cooper's direction, Pagliano handled all software upgrades and general maintenance.<sup>51</sup> Cooper described his role as "the customer service face," and he could add users or reset passwords on the e-mail server.<sup>52</sup> Cooper and Pagliano both handled the acquisition and purchase of server-related items.<sup>53</sup> For example, in March 2009, Cooper registered a Secure Sockets Layer (SSL)<sup>1</sup> encryption certificate at Pagliano's direction for added security when users accessed their e-mail from various computers and devices.<sup>54,55</sup> Clinton stated she had no knowledge of the hardware, software, or security protocols used to construct and operate the servers.<sup>56</sup> When she experienced technical issues with her e-mail account she contacted Cooper for assistance in resolving those issues.<sup>57</sup>

(U//~~FOUO~~) Pagliano stated that a complete backup of the Pagliano Server was made on a Seagate external hard drive once a week and a differential backup<sup>m</sup> was completed every day, and this continued from the initial Pagliano Server installation in March 2009 until June 2011 when the external hard drive was replaced.<sup>58</sup> As space on the hard drive ran out, backups were deleted on a "first in, first out" basis.<sup>59</sup> In June 2011, Pagliano replaced the Seagate external hard drive with a Cisco Network Attached Storage (NAS) device, to store backups of the server.<sup>60</sup> The FBI was unable to forensically determine how frequently the NAS captured backups of the Pagliano Server.

(U//~~FOUO~~) According to Pagliano, in early 2013, due to user limitations and reliability concerns regarding the Pagliano Server, staff for Clinton and President Clinton discussed future e-mail server options, and a search was initiated to find a vendor to manage a Clinton e-mail server<sup>n</sup>.<sup>61</sup> Additionally, Pagliano's expressed desire to seek new employment contributed to the decision to move to a new server.<sup>62</sup> A search for the new vendor was facilitated with the assistance of [REDACTED] Infograte, an information technology consulting company.<sup>63,64,65</sup> [REDACTED] was introduced to Clinton's Chief of Staff, Cheryl Mills, on or about January 2, 2013 through a mutual business associate.<sup>66</sup> [REDACTED] stated she worked with Mills and Pagliano to produce a request for proposal which was used to solicit responses from multiple firms, including Denver-based information technology firm Platte River Networks (PRN).<sup>67</sup> Clinton recalled that the transition to the PRN Server was initiated by President Clinton's aides seeking a higher level of service than could be provided by the Pagliano Server.<sup>68</sup> Pagliano identified President Clinton's [REDACTED] as making the final decision to select PRN.<sup>69</sup> In the spring of 2013, PRN negotiated the terms of the contract to host e-mail services and eventually signed a Service Level Agreement on July 18, 2013.<sup>70,71</sup>

b6  
b7Cb6  
b7C

<sup>1</sup> (U) SSL is a security protocol used to establish an encrypted connection between a server and another machine, allowing sensitive information such as login credentials or credit card information to be transmitted in an encrypted format instead of in plain text. SSL certificates, issued by a third-party Certificate Authority, are small files that must be installed on servers to establish secure sessions with web browsers.

<sup>m</sup> (U) A differential backup is a cumulative backup of all changes that have occurred since the last full backup.

<sup>n</sup> (U//~~FOUO~~) The new Clinton e-mail server hosted e-mail for Clinton, President Clinton, [REDACTED] and their respective staffs.

b6  
b7C

C. (U//~~FOUO~~) *Third E-mail Server: June 2013 – October 2015*

(U//~~FOUO~~) Following the selection of PRN to manage the Clintons' personal e-mail server and accounts, PRN's management assigned two PRN employees to handle the primary installation and administration of the third server system (PRN Server).<sup>74</sup> [redacted] who worked remotely from his home in [redacted] handled day-to-day administration for the PRN Server, and [redacted] who worked at PRN's headquarters in Colorado, handled all hardware installation and any required physical (i.e. "hands-on") maintenance for the PRN Server.<sup>75,76,77,78</sup> During the transition to the PRN Server, [redacted] advised he worked with Pagliano to understand the existing architecture of the Pagliano Server.<sup>74</sup> As part of this transition process, on or around June 4, 2013, [redacted] was granted administrator access to the Pagliano Server, as well as any accompanying services, such as the domain registration services through Network Solutions.<sup>75,76,77,78</sup>

b6  
b7C

(U//~~FOUO~~) On June 23, 2013, [redacted] traveled to Clinton's Chappaqua residence, where he powered down the Pagliano Server and transported it to a datacenter in Secaucus, New Jersey, run by Equinix, Inc. (Equinix).<sup>79,80,81</sup> The PRN Server remained at the Equinix facility until it was voluntarily produced to the FBI on October 3, 2015.<sup>82,83</sup> The only equipment [redacted] left at the Chappaqua residence was the existing firewall and switch, since PRN intended to purchase its own firewalls and switches.<sup>84</sup> [redacted] reconnected and powered on the equipment for the Pagliano Server at the datacenter, so users could connect to their e-mail accounts,<sup>85</sup> and he continued to work at the datacenter for a few days setting up the remaining equipment<sup>p</sup> for the PRN Server.<sup>86</sup> [redacted] completed all of the onsite work, while [redacted] worked remotely to get the server online.<sup>87</sup> After [redacted] left Secaucus, New Jersey, to travel back to PRN's headquarters, all physical pieces of hardware had been installed except for an intrusion detection device. [redacted] told the FBI that Equinix installed this device shortly after he left because the intrusion detection device was shipped later.<sup>88</sup>

b6  
b7C

(U//~~FOUO~~) On or around June 30, 2013, [redacted] began to remotely migrate all e-mail accounts from the Pagliano Server to the PRN Server.<sup>89</sup> During this migration period, the two server systems functioned together to ensure uninterrupted e-mail delivery to users.<sup>90</sup> After several days of migration, all e-mail accounts hosted on the presidentclinton.com, wjcoffice.com, and clintonemail.com domains were transferred to the PRN Server.<sup>q,91</sup> At that point, PRN kept the Pagliano Server online to ensure e-mail was still being delivered; however, the Pagliano Server was no longer hosting e-mail services for the Clintons.<sup>92</sup>

b6  
b7C

<sup>o</sup> (U//~~FOUO~~) A third PRN employee, [redacted] only handled a few tasks related to the administration of the server system until he left the company in the summer of 2015.

b6  
b7C

<sup>p</sup> (U//~~FOUO~~) The PRN Server consisted of the following equipment: a Dell PowerEdge R620 server hosting four virtual machines, including four separate virtual machines for Microsoft Exchange e-mail hosting, a BES for the management of BlackBerry devices, a domain controller to authenticate password requests, and an administrative server to manage the other three virtual machines, a Datto SIRIS 2000 to store onsite and remote backups of the server system, a CloudJacket device for intrusion prevention, two Dell switches, and two Fortinet Fortigate 80C firewalls.

<sup>q</sup> (U//~~FOUO~~) The [redacted] domain was also added to the PRN Server at a later date.

(U//~~FOUO~~) As part of the PRN Server environment, [REDACTED] told the FBI that he configured a backup device from Connecticut-based company Datto, Inc. (Datto), a Datto SIRIS 2000,<sup>r</sup> to take multiple snapshots of the server system daily, with a retention period of 60 days.<sup>93</sup> The backup device also made multiple copies of the Pagliano Server between June 24, 2013 and December 23, 2013.<sup>94</sup> At the Clintons' request, PRN only intended that the backup device store local copies of the backups.<sup>95,96</sup> However, in August 2015, Datto informed PRN that, due to a technical oversight, the PRN Server was also backing up the server to Datto's secure cloud storage.<sup>97,98</sup> After this notification, PRN instructed Datto to discontinue the secure cloud backups.<sup>99,100</sup>

b6  
b7C

(U//~~FOUO~~) [REDACTED] stated the Clintons originally requested that e-mail on the PRN Server be encrypted such that no one but the users could read the content.<sup>101</sup> However, PRN ultimately did not configure the e-mail settings this way to allow system administrators to troubleshoot problems occurring within user accounts.<sup>102</sup>

b6  
b7C

(U//~~FOUO~~) PRN utilized an Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) called CloudJacket from SECNAP Network Security.<sup>103</sup> The IDS/IPS device implemented by PRN had pre-configured settings that blocked or blacklisted certain e-mail traffic identified as potentially harmful and provided real-time monitoring, alerting, and incident response services.<sup>104,105</sup> SECNAP personnel would receive notifications when certain activity on the network triggered an alert.<sup>106</sup> These notifications were reviewed by SECNAP personnel and, at times, additional follow-up was conducted with PRN in order to ascertain whether specific activity on the network was normal or anomalous.<sup>107</sup> Occasionally, SECNAP would send e-mail notifications to [REDACTED] prompting him to block certain IP addresses.<sup>108</sup> [REDACTED] described these notifications as normal and did not recall any serious security incident or intrusion attempt.<sup>109</sup> PRN also implemented two firewalls for additional protection of the network. [REDACTED] stated that he put two firewalls in place for redundancy in case one went down.<sup>110</sup>

b6  
b7C

(U//~~FOUO~~) According to the FBI's forensic analysis of the server system, on December 3, 2013, Microsoft Exchange was uninstalled on the Pagliano Server.<sup>111</sup> The Pagliano Server remained in the same server cage at the Equinix datacenter in Secaucus, New Jersey, and a forensic review of the server, which was obtained in August 2015 via consent provided by Clinton through Williams & Connolly, indicated that it continued to be powered on and off multiple times before the FBI obtained it.<sup>112</sup> At the time of the FBI's acquisition of the Pagliano Server, Williams & Connolly did not advise the US Government (USG) of the existence of the additional equipment associated with the Pagliano Server, or that Clinton's clintonemail.com e-mails had been migrated to the successor PRN Server remaining at Equinix. The FBI's subsequent investigation identified this additional equipment and revealed the e-mail migration. As a result, on October 3, 2015, the FBI obtained, via consent provided by Clinton through Williams & Connolly, both the remaining Pagliano Server equipment and the PRN Server, which had remained operational and was hosting Clinton's personal e-mail account until it was disconnected and produced to the FBI.<sup>113,114,115,116</sup>

<sup>r</sup> (U) The Datto SIRIS 2000 is a device that provides back-up capability and data redundancy.

(U//~~FOUO~~) Investigation determined Clinton and Abedin began using new e-mail accounts on the domain hrcoffice.com in December 2014.<sup>111</sup> [redacted]

[redacted]<sup>118,119</sup> Abedin stated the clintonemail.com system was “going away” and, following the initiation of the new domain, Abedin did not have access to her clintonemail.com account.<sup>120</sup> [redacted]

b3  
b6  
b7C

[redacted]<sup>121,122</sup> This is consistent with representations made by Williams & Connolly, which stated in a February 22, 2016 letter: “Secretary Clinton did not transfer her clintonemail.com e-mails for the time period January 21, 2009 through February 1, 2013 to her hrcoffice.com account ...”<sup>123</sup> The investigation found no evidence Clinton's hrcoffice.com account contained or contains potentially classified information or e-mails from her tenure as Secretary of State. The FBI has, therefore, not requested or obtained equipment associated with Clinton's hrcoffice.com account.

D. (U//~~FOUO~~) *Mobile Devices Associated with Clinton's E-mail Server Systems*

(U//~~FOUO~~) Clinton stated she used a personal e-mail address and personal BlackBerry for both personal and official business and this decision was made out of convenience.<sup>124</sup> Abedin recalled that at the start of Clinton's tenure, State advised personal e-mail accounts could not be linked to State mobile devices and, as a result, Clinton decided to use a personal device in order to avoid carrying multiple devices.<sup>125</sup> [redacted]

b3  
b6  
b7C

[redacted]<sup>127</sup> Cooper stated that he was aware of Clinton using a second mobile phone number.<sup>s,128</sup> Cooper indicated Clinton usually carried a flip phone along with her BlackBerry because it was more comfortable for communication and Clinton was able to use her BlackBerry while talking on the flip phone.<sup>129</sup> Clinton believed 212-[redacted] was her primary BlackBerry phone number, and she did not recall using a flip phone during her tenure at State, only during her service in the Senate.<sup>t,130</sup> Abedin and Mills advised they were unaware of Clinton ever using a cellular phone other than the BlackBerry.<sup>131,132</sup>

b6  
b7C

(U//~~FOUO~~) FBI investigation identified 13 total mobile devices, associated with her two known phone numbers, 212-[redacted] and 212-[redacted] which potentially were used to send e-mails using Clinton's clintonemail.com e-mail addresses.<sup>133</sup> Investigation determined Clinton used in succession 11 e-mail capable BlackBerry mobile devices associated with 212-[redacted] eight of which she used during her tenure as Secretary of State.<sup>134</sup> Investigation identified Clinton used two e-mail capable mobile devices associated with 212-[redacted] after her tenure.<sup>u,135</sup> On

b6  
b7C

<sup>s</sup> (U//~~FOUO~~) During his interview with the FBI, Cooper was mistakenly shown “202-[redacted]” as the second phone number. Cooper recognized the phone number as Clinton's second number; however the correct phone number is 212-[redacted]

<sup>t</sup> (U//~~FOUO~~) AT&T toll records associated with 212-[redacted] indicated the number was consistently used for phone calls in 2009 and then used sporadically through the duration of Clinton's tenure and the years following. Records also showed that no BlackBerry devices were associated with this phone number.

b6  
b7C

<sup>u</sup> (U//~~FOUO~~) The FBI identified four additional mobile devices associated with 212-[redacted] which were used during Clinton's tenure. However, these devices lacked e-mail capability, and as a result the FBI did not conduct any further investigation regarding these devices.

February 9, 2016, DOJ requested all 13 mobile devices from Williams & Connolly.<sup>136</sup> Williams & Connolly replied on February 22, 2016 that they were unable to locate any of these devices.<sup>137</sup> As a result, the FBI was unable to acquire or forensically examine any of these 13 mobile devices.

(U//~~FOUO~~) On October 16, 2015, Williams & Connolly provided two other BlackBerry devices to the FBI and indicated the devices might contain or have previously contained e-mails from Clinton's personal e-mail account during her tenure as Secretary of State.<sup>v, 138, 139</sup> FBI forensic analysis found no evidence to indicate either of the devices provided by Williams & Connolly were connected to one of Clinton's personal servers or contained e-mails from her personal accounts during her tenure.<sup>140, 141, 142</sup>

(U//~~FOUO~~) The FBI identified five iPad devices associated with Clinton which potentially were used to send e-mails from Clinton's clintonemail.com e-mail addresses.<sup>143, 144, 145, 146</sup> The FBI obtained three of the iPads.<sup>147, 148, 149</sup> One iPad contained three e-mails from 2012 in the hdr22@clintonemail.com "drafts" folder.<sup>150</sup> The FBI assessed the three e-mails did not contain potentially classified information.<sup>151</sup> The FBI did not recover e-mails from Clinton's personal e-mail accounts from either of the other two iPads in its possession.<sup>152</sup>

(U//~~FOUO~~) Monica Hanley, a former Clinton aide, often purchased replacement BlackBerry devices for Clinton during her tenure at State.<sup>153</sup> Hanley recalled purchasing most of the BlackBerry devices for Clinton from AT&T stores located in the Washington, D.C. area.<sup>154</sup> Whenever Clinton acquired new mobile devices, Cooper was usually responsible for setting up the new devices and syncing them to the server.<sup>155</sup> Abedin, [REDACTED] and Hanley also assisted Clinton with setting up any new devices.<sup>156</sup> According to Abedin, it was not uncommon for Clinton to use a new BlackBerry for a few days and then immediately switch it out for an older version with which she was more familiar.<sup>157</sup> Clinton stated that when her BlackBerry device malfunctioned, her aides would assist her in obtaining a new BlackBerry, and, after moving to a new device, her old SIM cards were disposed of by her aides.<sup>158</sup> Cooper advised he sometimes assisted users, including Clinton, when they obtained a new mobile device by helping them back up the data from the old device before transferring it to the new device and syncing the new device with Clinton's server.<sup>159</sup> Abedin and Hanley indicated the whereabouts of Clinton's devices would frequently become unknown once she transitioned to a new device.<sup>160, 161</sup> Cooper did recall two instances where he destroyed Clinton's old mobile devices by breaking them in half or hitting them with a hammer.<sup>162</sup>

## **2. (U//~~FOUO~~) Clinton's Handling of E-mail and Classified Information**

### ***A. (U//~~FOUO~~) Clinton's Decision To Use Personal E-mail and Server Systems***

(U//~~FOUO~~) FBI investigation determined the State Executive Secretariat's Office of Information Resource Management (S/ES-IRM) offered Clinton a State e-mail address at the start of her

---

<sup>v</sup> (U//~~FOUO~~) The mobile devices provided to the FBI from Williams & Connolly on October 16, 2015 did not contain SIM cards or Secure Digital (SD) cards.

tenure; however, Clinton's staff<sup>w</sup> declined the offer.<sup>163</sup> According to [redacted]  
[redacted] State S/ES-IRM, Clinton was offered a State e-mail address, but instead decided to use the personal server from her 2008 presidential campaign.<sup>x,164</sup> Investigation identified the existence of two State-issued e-mail accounts associated with Clinton; however, these accounts were used on Clinton's behalf and not by Clinton herself. According to State, SMSGs@state.gov was used to send e-mail messages from the Secretary to all State employees.<sup>165,166</sup> This account was not configured to receive e-mails, and S/ES-IRM authored the messages sent from this account.<sup>167</sup> S/ES-IRM created SSHRC@state.gov to manage an Outlook calendar for Clinton, but this account was not configured to send or receive e-mails other than calendar invitations.<sup>168,169</sup> A May 25, 2016 report issued by the State Office of Inspector General (OIG)<sup>y</sup> stated that, during Clinton's tenure as Secretary of State, the State Foreign Affairs Manual (FAM) required day-to-day operations at State be conducted using an authorized information system.<sup>170</sup> The OIG stated it found "no evidence" that Clinton sought approval to conduct State business via her personal e-mail account or private servers, despite her obligation to do so.<sup>171</sup> Clinton told the FBI that she did not explicitly request permission from State to use a private server or e-mail address.<sup>172</sup> According to the State OIG report, State employees alleged that John Bentel, then-Director of S/ES-IRM, discouraged employees from raising concerns about Clinton's use of personal e-mail.<sup>z,173</sup> When interviewed by the FBI, Bentel denied that State employees raised concerns about Clinton's e-mail to him, that he discouraged employees from discussing it, or that he was aware during Clinton's tenure that she was using a personal e-mail account or server to conduct official State business.<sup>174</sup>

b6  
b7C

(U//~~FOUO~~) The FBI investigation determined some Clinton aides and senior-level State employees were aware Clinton used a personal e-mail address for State business during her tenure. Clinton told the FBI it was common knowledge at State that she had a private e-mail address because it was displayed to anyone with whom she exchanged e-mails.<sup>175</sup> However, some State employees interviewed by the FBI explained that e-mails from Clinton only contained the letter "H" in the sender field and did not display her e-mail address.<sup>176,177,178</sup> The majority of the State employees interviewed by the FBI who were in e-mail contact with Clinton indicated they had no knowledge of the private server in her Chappaqua residence.<sup>179,180,181,182,183,184</sup> Clinton's immediate aides, to include Mills, Abedin, Jacob Sullivan,<sup>aa</sup> and [redacted] told the FBI they were unaware of the existence of the private server until after Clinton's tenure at State or when it became public knowledge.<sup>185,186,187,188</sup>

b6  
b7C

<sup>w</sup> (U//~~FOUO~~) S/ES-IRM employees interviewed indicated they did not communicate directly with Clinton regarding this issue and could not specifically identify the members of Clinton's immediate staff with whom they spoke.

<sup>x</sup> (U//~~FOUO~~) According to [redacted] part of his job at State was to maintain and support the infrastructure for the UNCLASSIFIED and SECRET networks for the Executive Secretariat.

b6  
b7C

<sup>y</sup> (U//~~FOUO~~) Independent of the FBI's investigation, in April 2015, the State OIG initiated its own investigation and review of records management policies and practices regarding the use of non-State communications systems during the tenure of five Secretaries of State, including Clinton. Portions of the State OIG's May 25, 2016 report relevant to the FBI's investigation are cited herein.

<sup>z</sup> (U) According to the State OIG report, two State information management staff members approached the Director of the S/ES-IRM in 2010 with concerns they had about Clinton's use of a personal e-mail account and compliance with federal records requirements. According to one staff member, the Director stated that Clinton's personal system had been reviewed and approved by State legal staff. The Director allegedly told both staff members never to discuss Clinton's personal e-mail system again. OIG found no evidence that State legal staff reviewed or approved Clinton's personal e-mail system.

<sup>aa</sup> (U) Sullivan served as the Deputy Chief of Staff and later the Director of Policy and Planning during Clinton's tenure as Secretary of State.



(U//~~FOUO~~) The FBI investigation indicated Clinton was aware her use of a personal device, e-mail account, and server did not negate her obligation to preserve federal records. On January 23, 2009, Clinton contacted former Secretary of State Colin Powell via e-mail to inquire about his use of a BlackBerry while he was Secretary of State (January 2001 to January 2005).<sup>bb,189</sup> In his e-mail reply, Powell warned Clinton that if it became "public" that Clinton had a BlackBerry, and she used it to "do business," her e-mails could become "official record[s] and subject to the law."<sup>190</sup> Powell further advised Clinton, "Be very careful. I got around it all by not saying much and not using systems that captured the data."<sup>191</sup> Clinton indicated to the FBI that she understood Powell's comments to mean any work-related communications would be government records, and she stated Powell's comments did not factor into her decision to use a personal e-mail account.<sup>192</sup> In an e-mail to Mills on August 30, 2011, State Executive Secretary, Stephen Mull, cited a request from Clinton to replace her temporarily malfunctioning personal BlackBerry with a State-issued device.<sup>193</sup> Mull informed Mills that a State-issued replacement device for Clinton's personal BlackBerry would be subject to FOIA requests.<sup>194</sup> On that same day, Bentel sent a separate e-mail to Hanley, which was later forwarded to Abedin, stating that e-mails sent to a State e-mail address for Clinton would be "subject to FOIA searches."<sup>195</sup> A State-issued device was not ultimately issued to Clinton; in her FBI interview, Abedin stated she felt it did not make sense to temporarily issue Clinton a State BlackBerry because it would have required significant effort to transfer all of her e-mails and contacts to a device that she would have only used for a few days.<sup>196</sup> The Mull and Bentel e-mails to Mills and Hanley did not indicate that transferring e-mail and/or contacts from Clinton's clintonemail.com account would be necessary to issue her a State BlackBerry.<sup>197,198,199</sup> Abedin stated she always assumed all of Clinton's communications, regardless of the account, would be subject to FOIA if they contained work-related material.<sup>200</sup>

(U//~~FOUO~~) While State policy during Clinton's tenure required that "day-to-day operations [at State] be conducted on [an authorized information system],"<sup>201</sup> according to the [REDACTED] the Bureau of Information Security Management, [REDACTED] there was no restriction on the use of personal email accounts for official business.<sup>202</sup> However, State employees were cautioned about security and records retention concerns regarding the use of personal e-mail. In 2011, a notice to all State employees was sent on Clinton's behalf, which recommended employees avoid conducting State business from personal e-mail accounts due to information security concerns.<sup>203</sup> Clinton stated she did not recall this specific notice, and she did not recall receiving any guidance from State regarding e-mail policies outlined in the State FAM.<sup>204</sup> Interviews with two State employees determined that State issued guidance which required employees who used personal e-mail accounts for State business to forward those work-related e-mails to their official State account for record-keeping purposes.<sup>205,206</sup> Investigation determined that State used the State Messaging and Archive Retrieval Toolset (SMART), which allows employees to electronically tag e-mails to preserve a record copy.<sup>207,208,209</sup> According to [REDACTED] then State's [REDACTED] SMART was developed to automate and streamline the process for archiving records.<sup>210</sup> According to the

b6  
b7Cb6  
b7C

<sup>bb</sup> (U) According to the State OIG report, when Powell arrived at State in 2001, the official unclassified e-mail system in place only permitted communication among State employees; therefore, Powell requested the use of a private line for his America Online (AOL) e-mail account to communicate with individuals outside of State. Prior to Powell's tenure, State employees did not have Internet connectivity on their desktop computers. During Powell's tenure, State introduced unclassified desktop external e-mail capability on a system known as OpenNet.



State OIG Report, IRM introduced SMART throughout State in 2009; however, the Office of the Secretary elected not to use the SMART system to preserve e-mails, partly due to concerns that the system would “allow overly broad access to sensitive materials.”<sup>211</sup> [redacted] told the FBI that representatives from the Executive Secretariat asked to be the last to receive the SMART rollout, and ultimately SMART was never rolled out to the Executive Secretariat Office.<sup>212</sup> This left the “print and file” method as the only approved method by which the Office of the Secretary could preserve record e-mails.<sup>213</sup>

(U//~~FOUO~~) Mills wrote in a letter to State, dated December 5, 2014, that it was Clinton's practice to e-mail State officials at their government e-mail accounts for official business, and, therefore, State already had records of Clinton's e-mails preserved within State recordkeeping systems.<sup>214</sup> Abedin also stated in her FBI interview that Clinton's staff believed relevant e-mails would be captured and preserved by State if any of the senders or recipients were using an official State e-mail account.<sup>215</sup> The State OIG stated in its report that this was not an appropriate method of preserving record e-mails, and Clinton should have preserved any record e-mails created and received on her personal account by printing and filing the e-mails in the Office of the Secretary.<sup>216</sup> State OIG also determined Clinton should have surrendered all e-mails relating to State business before leaving her post as Secretary of State.<sup>217</sup> Clinton stated that she received no instructions or direction regarding the preservation or production of records from State during the transition out of her role as Secretary of State in early 2013.<sup>218</sup> Furthermore, Clinton believed her work-related e-mails were captured by her practice of sending e-mails to State employees' official State e-mail accounts.<sup>219</sup>

B. (U//~~FOUO~~) *Communications Equipment in Clinton's State Office and Residences*

(U//~~FOUO~~) Investigation determined Clinton did not have a computer in her State office, which was located in a Sensitive Compartmented Information Facility (SCIF) on the seventh floor of State headquarters, in an area often referred to as “Mahogany Row.”<sup>220,221,222</sup> State Diplomatic Security Service (DS) instructed Clinton that because her office was in a SCIF, the use of mobile devices in her office was prohibited.<sup>223</sup> Interviews of three former DS agents revealed Clinton stored her personal BlackBerry in a desk drawer in DS “Post 1,”<sup>cc</sup> which was located within the SCIF on Mahogany Row.<sup>224,225,226</sup> State personnel were not authorized to bring their mobile devices into Post 1, as it was located within the SCIF.<sup>227</sup> According to Abedin, Clinton primarily used her personal BlackBerry or personal iPad for checking e-mails, and she left the SCIF to do so, often visiting State's eighth floor balcony.<sup>228</sup> Former Assistant Secretary of State for DS Eric Boswell stated he never received any complaints about Clinton using her personal BlackBerry inside the SCIF.<sup>229</sup>

(S//~~OC/NF~~) [redacted]

[redacted] This decision was relayed to Clinton's executive staff via a memo titled “Use of Blackberries in Mahogany Row,” dated March 6, 2009.<sup>232</sup> Clinton stated to the FBI that she requested a secure BlackBerry while at State after hearing President Obama had one, but she

(U) <sup>cc</sup> (S//~~OC/NF~~) The DS security detachment maintained a Post, known as Post 1, located in the SCIF and directly outside of Clinton's office on Mahogany Row.

could not recall the reasons why State was unable to fulfill this request.<sup>dd,233</sup> Early in Clinton's tenure at State, Clinton's executive staff also inquired about the possibility of the Secretary using an iPad to receive communications in her office; however, this request was also denied due to restrictions associated with the Secretary's office being in a SCIF.<sup>234</sup> According to the State OIG report, in January 2009, in response to Clinton's desire to take her BlackBerry into secure areas, Mills discussed with S/ES-IRM officials and with the State Under Secretary for Management, Patrick Kennedy, alternative solutions which would allow Clinton to check e-mail from her desk.<sup>235</sup> Setting up an Internet-connected, stand-alone computer was discussed as a viable solution; however, a stand-alone system was never set up.<sup>236</sup>

(U) ~~(S//OC/NF)~~ Investigation determined Clinton had access to a number of State-authorized secure means of telephonic communication in her residences and in her office at State.<sup>ee,237</sup> At the start of Clinton's tenure, State installed a SCIF and secure communications equipment. [redacted]

b1  
b3

(S) [redacted] in her residences in Washington, D.C. (Whitehaven residence) and Chappaqua.<sup>ff,gg,hh,238,239,240,241,242</sup> According to Abedin, Cooper, and [redacted] there were personally-owned desktop computers in the SCIFs in Whitehaven and Chappaqua.<sup>243,244,245</sup> Conversely, Clinton stated to the FBI she did not have a computer of any kind in the SCIFs in her residences.<sup>246</sup> According to Abedin and Clinton, Clinton did not use a computer, and she primarily used her BlackBerry or iPad for checking e-mails.

b6  
b7C

C. (U//~~FOUO~~) *Individuals in Direct Communication with Clinton's Personal E-mail Address*

(U//~~FOUO~~) Investigation determined a limited number of individuals maintained direct e-mail contact with Clinton through her personal clintonemail.com e-mail account during her tenure at State. Thirteen individuals, consisting of State senior-level employees, work-related advisors, and State executive administrative staff, maintained direct e-mail contact with Clinton and individually e-mailed her between 100 and 1,000 times during her tenure.<sup>ii</sup> Abedin, Mills, and Sullivan, were most frequently in e-mail contact with Clinton and accounted for 68 percent of the e-mails sent directly to Clinton. In addition to sending Clinton messages they wrote, Abedin, Mills, and Sullivan reviewed e-mails they received from other State employees, USG contacts, and foreign government contacts, and if deemed appropriate they then forwarded the information

(U) ~~(S//OC/NF)~~ According to Clinton, her request for a State-issued secure BlackBerry was not out of concern for the sensitivity of the information on the device she was using at the time, rather she wanted the secure device to deal with future contingencies.

b1  
b3

<sup>ee</sup> (S//~~OC/NF~~) According to Abedin, Clinton's State office contained [redacted]

b6

<sup>ff</sup> (U//~~FOUO~~) According to Abedin, the SCIF door at the Whitehaven residence was not always locked, and Abedin, Hanley, and [redacted] had access to the SCIF.

b7C

(U) ~~(S//OC/NF)~~ Investigation determined the Chappaqua SCIF was not always secured, and Abedin, Hanley, and [redacted] had routine access to the SCIF.

b6  
b7C

<sup>hh</sup> (S//~~OC/NF~~) On [redacted] State installed the following communications lines at the Whitehaven residence [redacted]

[redacted] State installed communications equipment at the Chappaqua residence similar to that at the Whitehaven residence. State finished installation of the SCIF in the Chappaqua residence in [redacted]

b1

b3

<sup>ii</sup> (U//~~FOUO~~) The statistics in this paragraph are based on the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI, excluding Clinton's personal correspondence with family and close friends, as well as e-mails Clinton forwarded to herself.

to Clinton.<sup>247,248,249</sup> Multiple State employees advised they considered e-mailing Abedin, Mills, and Sullivan the equivalent of e-mailing Clinton.<sup>250,251</sup>

(U//~~FOUO~~) Investigation identified hundreds of e-mails sent by Abedin and other State staff to [redacted] presidentclinton.com e-mail address requesting him to print documents for Clinton. Some of these e-mails were determined to contain information classified at the CONFIDENTIAL level.<sup>ij,252,253,254,255,256,257</sup> [redacted] received a security clearance at the SECRET level on October 25, 2007 from the Department of Defense (DOD).<sup>258</sup> Documentation retained by DOD and provided to the FBI did not indicate [redacted] security clearance was deactivated upon his retirement from the US Navy Reserves in September 2010.<sup>259</sup>

b6  
b7C

D. (U//~~FOUO~~) *Clinton Staff's Use of Personal E-mail Accounts for Official Business*

(U//~~FOUO~~) Clinton's immediate staff, to include Mills, Sullivan, Abedin, [redacted] and Hanley, told the FBI in interviews that they predominantly used their State-provided OpenNet e-mail accounts to conduct official State business.<sup>260,261,262,263,264</sup> Exceptions to this practice included instances when the State OpenNet e-mail system was down or when staff was traveling internationally and OpenNet was not readily accessible.<sup>265,266,267,268,269</sup> The FBI's investigation confirmed that Clinton's immediate staff used their personal e-mail accounts in combination with their State-provided OpenNet e-mail accounts for official State business.<sup>kk</sup>

b6  
b7C

E. (U//~~FOUO~~) *Clinton's Use of Personal E-mail Accounts While Overseas*

(U//~~FOUO~~) FBI investigation and the State OIG report determined that State issued regular notices to staff during Clinton's tenure highlighting cybersecurity threats and advising that mobile devices must be configured to State security guidelines.<sup>270,271</sup> Clinton and her immediate staff were notified of foreign travel risks and were warned that digital threats began immediately upon landing in a foreign country, since connection of a mobile device to a local network provides opportunities for foreign adversaries to intercept voice and e-mail transmissions.<sup>272,273</sup> The State Mobile Communications (MC) Team was responsible for establishing secure mobile voice and data communications for Clinton and her team when they were traveling domestically and abroad.<sup>274,275</sup> When the security climate required, the State MC was capable of [redacted]

b1  
b3

[redacted] could be received and viewed by Clinton and/or her designated staff.<sup>276,277</sup>

(S//~~OC/NF~~) Investigation determined that of the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI, approximately [redacted] e-mails were sent or received by Clinton on her personal e-mail accounts while she was traveling outside the continental United States (OCONUS) on official State business.<sup>ll,278</sup> [redacted]

b1  
b3

<sup>ij</sup> (U//~~FOUO~~) Investigation identified six e-mail chains forwarded to [redacted] that were determined from the State FOIA review to contain CONFIDENTIAL information. Five were forwarded by Abedin, and one was from Clinton.

<sup>kk</sup> (U) See Section 3.C for discussion of classified e-mails contained in Clinton's staff's personal e-mail accounts.

<sup>ll</sup> (U//~~FOUO~~) State listed Clinton's overseas travel by individual days, but did not provide additional information such as arrival and departure times. As a result, the FBI could not determine specifically which e-mails were sent while she was on the ground OCONUS versus in flight.

b6  
b7C

(S)

[redacted] FBI investigation determined that hundreds of e-mails classified CONFIDENTIAL during the State FOIA process were sent or received by Clinton while she was OCONUS. Approximately [redacted] e-mails were sent or received by Clinton [redacted]. On [redacted] occasions while OCONUS, Clinton had direct e-mail contact with an e-mail address for President Barack Obama. Of the [redacted] e-mails between Clinton and President Obama, [redacted] were sent and received [redacted]. None of these [redacted] e-mails were determined to contain classified information. Clinton told the FBI that she received no particular guidance as to how she should use President Obama's e-mail address, and the e-mails sent while Clinton was [redacted] nm, 279

b1  
b3

F. (U//~~FOUO~~) Clinton's Production of E-mail in Response to FOIA and Other Requests

(U//~~FOUO~~) The House Select Committee on Benghazi was established on May 8, 2014 and reached an agreement with State on July 23, 2014 regarding the production of records.<sup>280</sup> State sent a formal request to former Secretaries of State on October 28, 2014, asking them to produce e-mails related to their government work.<sup>281</sup> After State requested that Clinton provide her e-mails,<sup>nm</sup> Clinton asked her attorneys, David Kendall<sup>oo</sup> and Mills, to oversee the process of providing Clinton's work-related e-mails to State.<sup>282</sup> Heather Samuelson,<sup>pp</sup> an attorney working with Mills, undertook a review to identify work-related e-mails, while Kendall and Mills oversaw the process.<sup>283</sup> Ultimately, on December 5, 2014, Williams & Connolly provided approximately 55,000 pages of e-mails<sup>qq</sup> to State in response to State's request for Clinton to produce all e-mail in her possession that constituted a federal record from her tenure as Secretary of State.<sup>284</sup> State ultimately reviewed the 55,000 pages of e-mail to meet its production obligations related to FOIA lawsuits and requests. On May 27, 2015, State received a court order to post Clinton's e-mails to the State FOIA website on a monthly production schedule with a completion date of January 29, 2016.<sup>285</sup> State ultimately concluded its FOIA-related production on February 29, 2016. Clinton told the FBI that she directed her legal team to provide any work-related or arguably work-related e-mails to State; however she did not participate in the development of the specific process to be used or in discussions of the locations of where her e-mails might exist.<sup>286</sup> Clinton was not consulted on specific e-mails in order to determine if they were work-related.<sup>287</sup>

<sup>nm</sup> (S//~~OC/NF~~) [redacted]b1  
b3

<sup>nn</sup> (U//~~FOUO~~) During the summer of 2014, State indicated to Mills a request for Clinton's work-related e-mails would be forthcoming, and in October 2014, State followed up by sending an official request to Clinton asking for her work-related e-mails.

<sup>oo</sup> (U) Kendall is a partner at Williams & Connolly.

<sup>pp</sup> (U) Samuelson worked in the White House Liaison Office at State during Clinton's tenure and currently serves as Clinton's personal attorney.

<sup>qq</sup> (U//~~FOUO~~) According to Clinton's campaign website, 30,490 potentially work-related e-mails were provided to State on December 5, 2014. On August 6, 2015, Williams & Connolly provided the FBI a .PST file containing 30,542 e-mail related files, which included 30,524 e-mail messages.

(U//~~FOUO~~) In July 2014, to initiate the review of Clinton's e-mails for production to State, Mills arranged for [redacted] to export from the PRN Server all of Clinton's e-mails sent to or received from a .gov e-mail address during Clinton's tenure as Secretary of State.<sup>288,289,290</sup> Once [redacted] completed this export from the PRN Server, he remotely transferred a .PST file containing the e-mails onto Mills's and Samuelson's laptops via ScreenConnect.<sup>rr,291,292,293</sup> In late September 2014, Mills and Samuelson asked [redacted] to provide a full export of all of Clinton's e-mails from her tenure, to include e-mails sent to and received from non-.gov e-mail addresses.<sup>294,295,296</sup> Mills and Samuelson explained that this follow-up request was made to ensure their review captured all of the relevant e-mails from Clinton's tenure.<sup>297,298</sup> [redacted] completed this export and transfer in the same manner as the July 2014 request.<sup>ss</sup> Mills and Samuelson did not know from what location on the server [redacted] extracted Clinton's e-mails.<sup>299,300</sup> [redacted] gave the FBI inconsistent statements over the course of three interviews regarding from where on the server he extracted Clinton's e-mails, and FBI investigation and forensic analysis have been unable to specifically identify the location and composition of the repository [redacted] used to create the export of Clinton's e-mails from her tenure.<sup>301,302,303</sup>

b6  
b7C

(U//~~FOUO~~) The FBI interviewed Samuelson on May 24, 2016 about her review of the PRN-provided e-mails. Samuelson indicated she conducted the review of these e-mails over the course of several months and completed it just prior to December 5, 2014, when hard copies of the work-related e-mails were turned over to State.<sup>304</sup> Using her laptop to conduct the review, Samuelson placed any work-related e-mails into a folder that she had created in Microsoft Outlook.<sup>305</sup> Samuelson first added to this folder all e-mails sent to or from Clinton's personal e-mail account with .gov and .mil e-mail addresses.<sup>306</sup> Samuelson then searched the remaining e-mails for the names of State senior leadership, as well as any members of Congress, foreign leaders, or other official contacts.<sup>307</sup> Finally, Samuelson conducted a key word search of terms such as "Afghanistan," "Libya," and "Benghazi."<sup>tt,308</sup> Samuelson reviewed the "To," "From," and "Subject" fields of every e-mail during this review; however, she did not read the content of each individual e-mail, indicating that, in some instances, she made a determination as to whether it was one of Clinton's work or personal e-mails by only reviewing the "To," "From," and "Subject" fields of the e-mail.<sup>309</sup>

(U//~~FOUO~~) As she completed the review, Samuelson printed all of the e-mails to be turned over to State using a printer in Mills's office.<sup>310</sup> According to Samuelson, Mills and Kendall subsequently reviewed e-mails that Samuelson printed, and any hard copy of an e-mail Mills and Kendall deemed not to be work-related was shredded, and the digital copy of the e-mail was not included in the folder Samuelson created in Microsoft Outlook to contain all of the work-related e-mails.<sup>311</sup> Mills stated that, other than instances where Samuelson requested Mills's guidance, Mills did not review the e-mails Samuelson identified as work-related, and once the review was complete, Samuelson printed the work-related e-mails.<sup>312</sup> After the review was completed, Samuelson created a .PST file containing all of the work-related e-mails and ensured that all work-related e-mails were printed.<sup>313</sup> This .PST file was provided to Kendall on a USB thumb

<sup>rr</sup> (U) ScreenConnect is a remote support administration tool that allows technicians to remotely connect to customers via a central web application to control and view end users' machines. According to product specifications, ScreenConnect encrypts data transmitted from one machine to another, to include screen data, file transfers, key strokes, and chat messages.

<sup>ss</sup> (U//~~FOUO~~) Mills did not recall if this second .PST file was transferred to her computer.

<sup>tt</sup> (U//~~FOUO~~) The FBI was unable to obtain a complete list of keywords or named officials searched from Samuelson, Mills, or Clinton's other attorneys due to an assertion of privilege.

drive.<sup>314</sup> On August 6, 2015, this thumb drive was obtained by the FBI from Williams & Connolly via consent from Clinton.

G. (U//~~FOUO~~) *Deletion of E-mail Associated with Clinton's Personal E-mail Accounts*

(U//~~FOUO~~) According to Hanley, in spring 2013, Cooper assisted Hanley in creating an archive of Clinton's e-mails.<sup>315</sup> Cooper provided Hanley with an Apple MacBook laptop (the Archive Laptop)<sup>uu</sup> from the Clinton Foundation and telephonically walked Hanley through the process of remotely transferring Clinton's e-mails from the Pagliano Server to the laptop and a thumb drive.<sup>316</sup> Hanley completed this task from her personal residence.<sup>317</sup> The two copies of the Clinton e-mail archive (one on the Archive Laptop and one on the thumb drive) were intended to be stored in Clinton's Chappaqua and Whitehaven residences; however, Hanley explained this did not occur as Hanley forgot to provide the Archive Laptop and the thumb drive to Clinton's staff following the creation of the archive.<sup>318,319</sup> In early 2014, Hanley located the Archive Laptop at her personal residence and worked with [REDACTED] to transfer the archive of Clinton's e-mails to PRN.<sup>320,321,322,323</sup> After trying unsuccessfully to remotely transfer the e-mails to [REDACTED]

b6  
b7C

[REDACTED] Hanley shipped the Archive Laptop to [REDACTED] residence in [REDACTED] in February 2014, and [REDACTED] migrated Clinton's e-mails from the Archive Laptop onto the PRN Server.<sup>324,325,326,327,328</sup> To accomplish this, [REDACTED] transferred all of the Clinton e-mail content to a personal Google e-mail (Gmail) address he created, [REDACTED]@gmail.com, and then downloaded all of the e-mail content from the Gmail account to a mailbox named "HRC Archive" with the e-mail address hrcarchive@clintonemail.com on the PRN Server.<sup>329,330,331</sup>

[REDACTED] advised he used the [REDACTED]@gmail.com e-mail account to facilitate the transfer because he had trouble exporting the e-mail from the Apple MacMail format to a format that would be compatible with Microsoft Exchange.<sup>332</sup>

(U//~~FOUO~~) Hanley stated she recommended that PRN wipe the Archive Laptop after the e-mails were transferred to the PRN Server.<sup>333</sup> However, [REDACTED] told the FBI that, after the transfer was complete, he deleted the e-mails from the Archive Laptop but did not wipe the laptop.<sup>334</sup> He also advised he deleted the e-mails uploaded to the [REDACTED]@gmail.com e-mail account per Hanley's instructions and shipped the Archive Laptop via United States Postal Service or United Parcel Service to [REDACTED] who was Clinton's [REDACTED] at the time.<sup>335,336,337</sup> [REDACTED] told the FBI that she never received the laptop from [REDACTED] however, she advised that Clinton's staff was moving offices at the time, and it would have been easy for the package to get lost during the transition period.<sup>338</sup> Neither Hanley nor [REDACTED] could identify the current whereabouts of the Archive Laptop or thumb drive containing the archive, and the FBI does not have either item in its possession.<sup>339</sup>

b6  
b7C

(U//~~FOUO~~) FBI investigation identified 940 e-mails associated with Clinton's personal e-mail account from October 25, 2010 to December 31, 2010 that as of June 21, 2016 remained within the [REDACTED]@gmail.com account.<sup>340</sup> The FBI was able to determine that 56 of these

b6  
b7C

<sup>uu</sup> (U//~~FOUO~~) According to Abedin, the archive of Clinton's e-mails was created as a reference for the future production of a book. According to Hanley, the archive of Clinton's e-mails was created in response to Clinton's [hdr22@clintonemail.com](mailto:hdr22@clintonemail.com) address being released to the public following the online posting of e-mail exchanges between Clinton and an informal political advisor, Sidney Blumenthal. Blumenthal's personal e-mail account, which contained his e-mails with Clinton, was compromised on March 14, 2013 by a Romanian cyber hacker. See Section 4.D.



e-mails have been identified as currently classified at the CONFIDENTIAL level through the State FOIA process.<sup>341</sup> Additionally, the FBI determined that 302 of the 940 e-mails identified in the [redacted]@gmail.com account were not found in the set of e-mails Clinton produced to State in December 2014.<sup>342</sup> Of the 302 e-mails, the FBI disseminated 18 to USG agencies for classification review. State determined one e-mail to be classified SECRET when sent and to be classified CONFIDENTIAL currently. State determined a second e-mail to be classified as CONFIDENTIAL when sent and to be currently UNCLASSIFIED.

b6  
b7C

(U//~~FOUO~~) In or around December 2014 or January 2015, Mills and Samuelson requested that [redacted] remove from their laptops all of the e-mails from the July and September 2014 exports.<sup>343,344,34</sup> [redacted] used a program called BleachBit<sup>vv</sup> to delete the e-mail-related files so they could not be recovered.<sup>346,347,34</sup> [redacted] remotely connected to Mills's and Samuelson's laptops via ScreenConnect to complete the deletions.<sup>349,350,35</sup> [redacted] stated to the FBI that an unknown Clinton staff member told him s/he did not want the .PST file after the export and wanted it removed from the PRN Server.<sup>352</sup> According to Mills, in December 2014, Clinton decided she no longer needed access to any of her e-mails older than 60 days.<sup>353</sup> Therefore, Mills instructed [redacted] to modify the e-mail retention policy on Clinton's clintonemail.com e-mail account to reflect this change.<sup>354</sup> However, according to [redacted] he did not make these changes to Clinton's clintonemail.com account until March 2015.<sup>355</sup> Clinton told the FBI that, after her staff completed her e-mail production to State in December 2014, she was asked what she wanted to do with her remaining personal e-mails, Clinton instructed her staff she no longer needed the e-mails.<sup>356</sup> Clinton stated she never deleted, nor did she instruct anyone to delete, her e-mails to avoid complying with FOIA, State or FBI requests for information.<sup>357</sup>

b6  
b7C

(U//~~FOUO~~) On March 2, 2015, *The New York Times* (NYT) published an article titled, "Hillary Clinton Used Personal Email Account at State Dept., Possibly Breaking Rules."<sup>ww,358</sup> This article identified publicly that Clinton exclusively used a personal e-mail account to conduct official State business while she was Secretary of State and had not produced her federal records to State until December 2014.<sup>359</sup> On March 3, 2015, the United States House Select Committee on Benghazi provided a letter to Williams & Connolly requesting the preservation and production of all documents and media related to hdr22@clintonemail.com and hrc17@clintonemail.com.<sup>xx,360</sup> The following day, the House Select Committee on Benghazi issued a subpoena to Clinton to produce e-mails from hdr22@clintonemail.com, hrod17@clintonemail.com, and other e-mail addresses used by Clinton, pursuant to the events surrounding the 2012 terrorist attack in Benghazi.<sup>361</sup>

(U//~~FOUO~~) In the days following the publication of the NYT article, Mills requested that PRN conduct a complete inventory of all equipment related to the Pagliano Server.<sup>362,363</sup> In response to this request, [redacted] traveled to the Equinix datacenter in Secaucus, New Jersey to conduct an onsite review of the equipment, while [redacted] also logged in to the server

b6  
b7C

<sup>vv</sup> (U) BleachBit is open source software that allows users to "shred" files, clear Internet history, delete system and temporary files and wipe free space on a hard drive. Free space is the area of the hard drive that can contain data that has been deleted. BleachBit's "shred files" function claims to securely erase files by overwriting data to make the data unrecoverable.

<sup>ww</sup> (U) The same article was released on the NYT website on March 2, 2015. The print version appeared on page A1 the following day, March 3, 2015.

<sup>xx</sup> (U) The House Select Committee on Benghazi submitted a preservation request for an accurate e-mail address, hdr22@clintonemail.com, and an inaccurate e-mail address, hrc17@clintonemail.com, for Clinton.



remotely.<sup>364,365,366</sup> [ ] powered on the Pagliano Server and confirmed for Mills that no additional data existed on any server equipment, as all data was migrated to the PRN Server.<sup>yy,367,368</sup>

b6  
b7C

(U//~~FOUO~~) Investigation indicated that on March 25, 2015, PRN held a conference call with President Clinton's staff.<sup>369,370</sup> In his interviews with the FBI, [ ] indicated that sometime between March 25-31, 2015, he realized he did not make the e-mail retention policy changes to Clinton's clintonemail.com e-mail account that Mills had requested in December 2014.<sup>371</sup> In his FBI interview on February 18, 2016, [ ] indicated that he did not recall conducting deletions based upon this realization.<sup>372</sup> In a follow-up FBI interview on May 3, 2016, [ ] indicated he believed he had an "oh shit" moment and sometime between March 25-31, 2015 deleted the Clinton archive mailbox from the PRN server and used BleachBit to delete the exported .PST files he had created on the server system containing Clinton's e-mails.<sup>373</sup> Investigation found evidence of these deletions<sup>374</sup> and determined the Datto backups of the PRN Server were also manually deleted during this timeframe.<sup>375</sup> Investigation identified a PRN work ticket, which referenced a conference call among PRN, Kendall, and Mills on March 31, 2015.<sup>376,377</sup> PRN's attorney advised [ ] not to comment on the conversation with Kendall based upon the assertion of the attorney-client privilege.<sup>378</sup>

b6  
b7C

(U//~~FOUO~~) Investigation identified a March 9, 2015 e-mail to PRN from Mills, of which [ ] was a recipient, referencing the preservation request from the Committee on Benghazi.<sup>379,380</sup> [ ] advised during his February 18, 2016 interview that he did not recall seeing the preservation request referenced in the March 9, 2015 e-mail.<sup>381</sup> During his May 3, 2016 interview, [ ] indicated that, at the time he made the deletions in March 2015, he was aware of the existence of the preservation request and the fact that it meant he should not disturb Clinton's e-mail data on the PRN Server.<sup>382</sup> [ ] also stated during this interview, he did not receive guidance from other PRN personnel, PRN's legal counsel, or others regarding the meaning of the preservation request.<sup>383</sup> Mills stated she was unaware that [ ] had conducted these deletions and modifications in March 2015.<sup>384</sup> Clinton stated she was also unaware of the March 2015 e-mail deletions by PRN.<sup>385</sup>

b6  
b7C

### **3. (U//~~FOUO~~) Results of FBI Review of Clinton E-mails Stored and Transmitted on Personal Server Systems**

#### ***A. (U//~~FOUO~~) Quantities of Clinton's E-mails Recovered from Personal Server Systems***

(U//~~FOUO~~) To date, the FBI has recovered from additional data sources and reviewed approximately 17,448 unique work-related and personal e-mails<sup>zz</sup> from Clinton's tenure containing Clinton's hdr22@clintonemail.com<sup>aaa</sup> e-mail address that were not provided by

<sup>yy</sup> (U//~~FOUO~~) FBI forensically identified deletions from the PRN Server on March 8, 2015 of .PST files not associated with Clinton's e-mail account or domain, and other server data.

<sup>zz</sup> (U//~~FOUO~~) These approximately 17,448 e-mails were determined to be unique from the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI, through a distinctive Internet Message ID. These files do not include documents or partial e-mail files without an Internet Message ID in the metadata.

<sup>aaa</sup> (U//~~FOUO~~) The approximate 17,448 e-mails may contain chains of e-mails in which Clinton is not on the most recent "To," "From," "CC," or "BCC" line.

Williams & Connolly as part of Clinton's production to the FBI, including e-mails from January 23, 2009 through March 18, 2009.<sup>bbb</sup>

*B. (U//~~FOUO~~) Classification Portion Markings in E-mail Recovered from Personal Server Systems*

(U//~~FOUO~~) The FBI identified three e-mail chains, encompassing eight individual e-mail exchanges to or from Clinton's personal e-mail accounts, which contained at least one paragraph marked "(C)," a marking ostensibly indicating the presence of information classified at the CONFIDENTIAL level.<sup>386,387,388</sup> The emails contained no additional markings, such as a header or footer, indicating that they were classified. State confirmed through the FOIA review process that one of these three e-mail chains contains information which is currently classified at the CONFIDENTIAL level.<sup>ccc,389</sup> State determined that the other two e-mail chains are currently UNCLASSIFIED.<sup>390,391</sup> State did not provide a determination as to whether any of these three e-mails were classified at the time they were sent.

(U//~~FOUO~~) When asked about the e-mail chain containing "(C)" portion markings that State determined to currently contain CONFIDENTIAL information, Clinton stated she did not know what the "(C)" meant at the beginning of the paragraphs and speculated it was referencing paragraphs marked in alphabetical order.<sup>ddd,392</sup> Clinton identified a "CONFIDENTIAL" header and footer (inserted in the document by the FBI prior to the interview) and asked if the "(C)" related to the "CONFIDENTIAL" header and footer.<sup>393</sup> Clinton did not believe the content of the e-mail was classified and questioned the classification determination.<sup>394</sup> When asked of her knowledge regarding TOP SECRET, SECRET, and CONFIDENTIAL classification levels of USG information, Clinton responded that she did not pay attention to the "level" of classification and took all classified information seriously.<sup>395</sup>

*C. (U//~~FOUO~~) Classified Information Found in Clinton's E-mails on Personal Server Systems*

(U//~~FOUO~~) FBI and USIC classification reviews identified 81 e-mail chains containing approximately 193 individual e-mail exchanges<sup>eee</sup> that were classified from the CONFIDENTIAL to TOP SECRET levels at the time the e-mails were drafted on UNCLASSIFIED systems and sent to or from Clinton's personal server. Of the 81 e-mail chains classified at the time of transmittal, 68 remain classified. Twelve of the e-mail chains, classified

<sup>bbb</sup> (U//~~FOUO~~) According to Clinton's campaign website, Clinton only provided State her work-related e-mails dated after March 18, 2009. E-mails from January 21, 2009 to March 18, 2009 were not produced to State or the FBI by Williams & Connolly. According to Samuelson and Mills, they were unable to locate Clinton's e-mails from this period. The e-mails from this time period were not provided to them by PRN, and they believed the e-mails were not backed up on any server. Investigation determined some of Clinton's e-mails from January 23, 2009 to March 17, 2009 were captured through a Datto backup on June 29, 2013. However, the e-mails obtained are likely only a subset of the e-mails sent or received by Clinton during this time period.

<sup>ccc</sup> (U//~~FOUO~~) The three e-mail chains containing the portion mark of "(C)" are not considered as part of the group of e-mails classified through the FBI classification review because State has not responded to the FBI request for classification determinations for these e-mails.

<sup>ddd</sup> (U//~~FOUO~~) Earlier in her FBI interview, when asked what the classification marking "(SBU)" meant, Clinton correctly stated Sensitive But Unclassified.

<sup>eee</sup> (U//~~FOUO~~) Due to the limited insight into other USG and personal e-mail accounts, the investigation was unable to determine if e-mails from the classified e-mail chains were forwarded to other USG or personal e-mail addresses.

by State as SECRET or CONFIDENTIAL, were not among the approximately 30,000 e-mails provided to State and the FBI by Williams & Connolly. In addition to State classified equities, the investigation determined the 81 e-mail chains contained classified equities from 5 other USIC agencies: the CIA, DOD, FBI, National Geospatial–Intelligence Agency (NGA), and National Security Agency (NSA).

(S//~~OC/NF~~) The 81 classified e-mail chains contained 8 e-mail chains classified TOP SECRET, 37 e-mail chains classified SECRET, and 36 e-mail chains classified CONFIDENTIAL at the time they were sent. Of these e-mail chains, 7 e-mail chains contained information associated with a Special Access Program (SAP) and 3 e-mail chains contained Sensitive Compartmented Information (SCI).<sup>fff</sup> Of the 81 classified e-mail chains, 36 e-mail chains were determined to be Not-Releasable to Foreign Governments (NOFORN) and 2 were considered releasable only to Five Allied partners (FVEY). [ ]

b1  
b3

[ ]  
Sixteen of the e-mail chains, classified at the time the e-mails were sent, were downgraded in current classification by USIC agencies.

(S//~~OC/NF~~) [ ]  
[ ]

- (S//~~OC/NF~~) [ ]

- (S//~~OC/NF~~) [ ]

- (S//~~OC/NF~~) [ ]

- (S//~~OC/NF~~) [ ]  
[ ]

b1  
b3

- (S//~~OC/NF~~) [ ]  
[ ]

- (S//~~OC/NF~~) [ ]  
[ ]

- (S//~~OC/NF~~) [ ]

- (S//~~OC/NF~~) [ ]  
[ ]

(U//~~FOUO~~) The State FOIA process identified 2,093 e-mails currently classified as CONFIDENTIAL or SECRET. Of these e-mails, FBI investigation identified approximately 100 e-mails that overlapped with the 193 e-mails (80 e-mail chains) determined through the FBI

<sup>fff</sup> (U//~~FOUO~~) One of the TOP SECRET/SCI e-mails was downgraded to a current classification of SECRET//REL TO USA, FVEY by the owning agency during a FOIA-related review.

classification review to be classified at the time sent. All except one of the remaining 2,093 e-mails were determined by the State FOIA process to be CONFIDENTIAL, with one e-mail determined to be SECRET at the time of the FOIA review.<sup>ggg,hhh</sup> State did not provide a determination as to whether the 2,093 e-mails were classified at the time they were sent.

(U//~~FOUO~~) The FBI investigation determined Clinton contributed to discussions in four e-mail chains classified as CONFIDENTIAL, three e-mail chains classified as SECRET//NOFORN, and four e-mail chains classified as TOP SECRET//SAP. Investigation identified 67 instances where Clinton forwarded e-mails to either State personnel or [redacted] for printing that were identified as classified CONFIDENTIAL or SECRET through either the State FOIA process or FBI classification determination requests.

b6  
b7C

(U//~~FOUO~~) FBI investigation determined at least 32 classified e-mail chains transited both the personal e-mail account of Clinton and the personal e-mail accounts of Abedin, Mills, Sullivan, or [redacted].<sup>iii</sup> One of these e-mails was TOP SECRET//SCI at the time of transmission, and is currently considered SECRET//REL TO USA, FVEY; five were classified as SECRET//NOFORN and one as SECRET both when sent and currently; two were classified SECRET when sent and are CONFIDENTIAL currently; one was classified as SECRET when sent and is UNCLASSIFIED//FOUO currently; 16 were classified CONFIDENTIAL both when sent and currently; five were CONFIDENTIAL when sent and UNCLASSIFIED//FOUO currently; and one was CONFIDENTIAL when sent and UNCLASSIFIED currently.<sup>iii</sup> Investigation determined at least 80 e-mails from the 2,093 e-mails deemed classified through the State FOIA process were sent to or from the personal accounts of Abedin, Mills, Sullivan, or [redacted].<sup>kk</sup>

b6  
b7C

*D. (U//~~FOUO~~) Witness Statements Related to Classified E-mails Found on Clinton's Personal Server Systems*

(U//~~FOUO~~) The FBI interviewed multiple officials who authored and/or contributed to e-mails, the content of which has since been determined to contain classified information.<sup>396,397,398,399,400,401,402,403,404,405,406,407,408</sup> USG employees responsible for initiating classified e-mail chains included State Civil Service employees, Foreign Service employees, Senior Executive Service employees, Presidential appointees, and non-State elected officials.

(U//~~FOUO~~) During FBI interviews, the authors of these e-mails provided context surrounding the e-mails in question as well as reasons for sending the e-mails on unclassified systems.

<sup>ggg</sup> (U//~~FOUO~~) Investigation determined the following types of e-mails were not included in the list of 2,093 e-mails classified through the State FOIA review: TS//SAP e-mails; e-mails not produced to State by Williams & Connolly; formerly classified e-mails now considered UNCLASSIFIED; and classified e-mails improperly released during FOIA production.

<sup>hhh</sup> (U//~~FOUO~~) Two attachments labeled as SECRET through State FOIA process were not tracked as separate classified documents in the FBI's classification review.

<sup>iii</sup> (U//~~FOUO~~) Due to the limited insight into other USG and personal e-mail accounts, FBI investigation was unable to determine if e-mails from classified e-mail chains were forwarded to other personal e-mail accounts.

<sup>iii</sup> (U//~~FOUO~~) In addition to the personal accounts of Abedin, Mills, Sullivan, and [redacted] seven classified e-mail chains were initially drafted in or sent from the private e-mail accounts of five non-State individuals, to include Kerry and Blumenthal.

<sup>kkk</sup> (U//~~FOUO~~) Personal e-mail accounts of Abedin, Mills, Sullivan, and [redacted] appeared in the "To," "From," or "CC" line of the e-mail. Investigation was not able to determine if additional personal accounts were blind carbon copied ("BCC").

b6  
b7C

Individuals who worked in the State Bureau of Public Affairs<sup>iii</sup> often accessed classified information to understand the context of unclassified information that was to be disseminated publicly.<sup>409</sup> The Public Affairs officials primarily relied upon reporting from country desk officers to generate talking points and believed the country desk officers were experienced in protecting sensitive information within their reporting.<sup>410</sup> The Public Affairs officials were also responsible for notifying State leadership of impending reports by the news media regarding sensitive or controversial topics.<sup>411</sup> Furthermore, a former DOD official explained that he sent an e-mail, since deemed to contain classified information, in order to quickly coordinate public affairs responses by State and DOD with respect to a specific incident referenced in the e-mail.<sup>412</sup>

(U//~~FOUO~~) Individuals, including those in the State Operations Center (Ops Center),<sup>mmmm</sup> who were responsible for passing information to high-level State officials, worked to identify and disseminate the information they deemed critical for review by State leadership.<sup>413,414</sup> These individuals noted that such information was generally sent on State unclassified e-mail systems because of the need to quickly elevate information at times when the intended recipients did not all have immediate access to classified e-mail accounts.<sup>nnn,415,416</sup>

(U//~~FOUO~~) Investigation identified seven e-mail chains comprised of 22 e-mails on Clinton's server classified by the USIC as TOP SECRET/SAP. State Department officials, both in Washington, D.C. and overseas, were briefed into the SAP and communicated both internally and with other USIC officials about the program.<sup>417,418,419,420</sup> Only internal State e-mails regarding the SAP were forwarded to Clinton, all of which were sent to Clinton's server by Sullivan. Clinton and Sullivan engaged in discussions regarding the SAP in four of the seven e-mail chains.

(S//~~OC/NF~~) During FBI interviews, State employees explained the context for why classified material [redacted] was sent and provided reasons to explain why they did not believe information in the e-mails was classified.<sup>421,422,423,424</sup> [redacted]

[redacted] stated that [redacted]

b1  
b3  
b6  
b7C

[redacted]<sup>427</sup> [redacted] stated the right method of communication was whichever method allowed for the fastest possible dissemination of the message.<sup>428</sup> He also stated that information he received from other USG agencies was "technically probably classified" but that "you can't do business

<sup>iii</sup> (U//~~FOUO~~) According to State's website, the Bureau of Public Affairs "engages domestic and international media to communicate timely and accurate information with the goal of furthering US foreign policy and national security interests as well as broadening understanding of American values."

<sup>mmmm</sup> (U//~~FOUO~~) The Ops Center is staffed 24 hours a day and constantly monitors reporting from State cables, other USG agencies, and open source news outlets for information of interest to State leadership.

<sup>nnn</sup> (U//~~FOUO~~) Individuals who inputted classified information into e-mail chains to pass to high-level State officials indicated that at times they were relying on information that others had summarized and provided to them.

that way.”<sup>429</sup> When interviewed by the FBI, authors of the e-mails stated that they used their best judgment in drafting the messages and that it was common practice at State to carefully word e-mails on UNCLASSIFIED networks so as to avoid sensitive details or “talk around” [redacted] classified information.<sup>430, 431, 432, 433</sup> [redacted] stated the information in the [redacted]

b1  
b3  
b6  
b7C

(S) [redacted] former [redacted] declined to comment on the e-mails.<sup>435</sup> [redacted] referenced news articles claiming e-mails on Clinton's server were over-classified, but after seeing the e-mails during the interview, stated he “now understood why people were concerned about this matter.”<sup>436</sup> Sullivan indicated he had no reason to believe any State employee ever intentionally mishandled classified information.<sup>437</sup>

(S//~~OC/NF~~) The FBI interviewed four USIC executives stationed both in the United States and overseas [redacted].<sup>438, 439, 440, 441</sup> The USIC executives reviewed the [redacted] e-mail chains which transited Clinton's personal e-mail account and assessed that some of the e-mail chains should be considered classified.<sup>442, 443, 444</sup> [redacted]

b1  
b3

[redacted]<sup>440</sup> However, two of the USIC executives interviewed said some of the [redacted]

(S//~~OC/NF~~) A majority of the USIC executives interviewed expressed concerns with how State handled [redacted].<sup>449, 450, 451</sup> According to a USIC executive who had been stationed overseas, State employees were aware of the sensitivities [redacted].<sup>452</sup>

b1  
b3

(U//~~FOUO~~) On April 9, 2016, Mills, who served as Chief of Staff to Clinton at State between 2009 and 2013, was interviewed by the FBI. During this interview, Mills was provided seven e-mails which contained information later determined to be classified. While Mills did not specifically remember any of the e-mails, she stated that there was nothing in them that concerned her regarding their transmission on an unclassified e-mail system.<sup>455</sup> Mills also stated that she was not concerned about her decision to forward certain of these e-mails to Clinton.<sup>456</sup> In reviewing e-mails related to the SAP referenced above, Mills explained that some of the e-mails were designed to inform State officials of media reports concerning the subject matter and that the information in the e-mails merely confirmed what the public already knew.<sup>457</sup>

(U//~~FOUO~~) The FBI interviewed Sullivan on February 27, 2016. Sullivan, who between 2009 and 2013 served at State first as the Deputy Chief of Staff for Policy and then as the Director of Policy Planning, communicated extensively with Clinton by e-mail. Their communications included both e-mails written by Sullivan and e-mails written by others that Sullivan forwarded to Clinton. During the interview, the FBI asked Sullivan to review approximately 14 e-mails Sullivan sent or received on unclassified systems that were later determined to contain classified information up to the TOP SECRET/SAP level. Sullivan did not specifically recall the e-mails, aside from recognizing some of them from the materials released pursuant to FOIA litigation, but

provided reasons why the e-mails may have been sent by him or others on unclassified systems.<sup>458</sup> With respect to the SAP, Sullivan stated that it was discussed on unclassified systems due to the operational tempo at that time, and State employees attempted to talk around classified information.<sup>459</sup> Sullivan also indicated that, for some of the e-mails, information about the incidents described therein may have already appeared in news reports.<sup>460</sup> Furthermore, Sullivan stated that his colleagues at State worked hard while under pressure and used their best judgment to accomplish their mission.<sup>461</sup> When forwarding e-mails, Sullivan relied on the judgment of the individuals who sent the e-mails to him to ensure that the e-mails did not contain classified information.<sup>462</sup> Sullivan did not recall any instances in which he felt uneasy about information conveyed on unclassified systems, nor any instances in which others expressed concerns about the handling of classified information at State.<sup>ooo,463</sup>

(S//~~OC/NF~~) Sullivan was also asked about an e-mail exchange between him and Clinton in which, on the morning of June 17, 2011, Clinton asked Sullivan to check on the status of talking points she was supposed to have received.<sup>464</sup> Sullivan responded that the secure fax was malfunctioning but was in the process of being fixed. Clinton instructed Sullivan that if the secure fax could not be fixed, he should "turn [the talking points] into nonpaper [with] no identifying heading and send nonsecure."<sup>465</sup> State uses the term "non-paper" to refer to a document which is authorized for distribution to a foreign government without explicit attribution to the U.S. government and without classified information. Sullivan did not recall this specific e-mail but believed that Clinton's request indicated that she would have wanted him to make an unclassified version of the document summarize the contents and then send it to her on a non-secure fax.<sup>466</sup>

b1  
b3

(U//~~FOUO~~) On April 5, 2016, Abedin, who served as Deputy Chief of Staff to Clinton at State between 2009 and 2013, was interviewed by the FBI. When asked about an e-mail subsequently determined to contain CONFIDENTIAL information, Abedin noted that she had only conveyed the information from the e-mail and had not originated it.<sup>470</sup> She also stated that she relied upon the sender to properly mark the e-mail for classification purposes and did not take it upon herself to question the sender's judgment as to such marking.<sup>ppp,471</sup>

(U//~~FOUO~~) Investigation determined Sidney Blumenthal, a former political aide to President Clinton and an informal political advisor to Clinton during her tenure at State, had direct e-mail contact with Clinton during her tenure at State. FBI investigation identified at least 179 e-

<sup>ooo</sup> (U//~~FOUO~~) Abedin and Mills also provided similar responses when asked about State security practices regarding classified information.

<sup>ppp</sup> (U//~~FOUO~~) Although Abedin was a party to e-mails containing information that has since been determined to be classified, due to the nature of her position at State, Abedin was not regularly included in the e-mail chains (discussed in this section of the memorandum) about which Sullivan and Mills were questioned. Abedin's position at State did not consistently involve her participation in substantive policy decisions, and she was not a regular user of classified e-mail systems.



mails<sup>qqq</sup> that Blumenthal sent to Clinton containing information in memorandum format. The State FOIA process identified 24 memos from Blumenthal that contained information currently classified as CONFIDENTIAL and one as SECRET both when sent and currently.<sup>472,473</sup> The FBI interviewed Blumenthal on January 7, 2016. According to Blumenthal, the content of the memos, which addressed topics to include Benghazi and foreign political developments, was provided to him from a number of different sources to include former USIC employees and contacts, as well as contacts within foreign governments.<sup>474,475,476,477,478,479,480,481,482,483,484,485,486,487</sup> The memos contained a notation of "CONFIDENTIAL"<sup>trr</sup> and then often included a source summary statement<sup>sss</sup> similar to those frequently found in USIC intelligence products.<sup>488,489,490</sup> Blumenthal indicated he was not tasked to provide this information to Clinton; rather, he provided it because he deemed the information helpful, which Clinton occasionally acknowledged via e-mail.<sup>491</sup> Clinton often forwarded the memos to Sullivan asking him to remove information identifying Blumenthal as the originator and to pass the information to other State employees to solicit their input.<sup>492,493</sup> According to e-mails between Clinton and Sullivan, Clinton discussed passing the information to the White House, other USG agencies, and foreign governments.<sup>ttt,494,495</sup>

*E. (U//~~FOUO~~) Clinton's Statements Related to Classified E-mails Found on Her Personal Server Systems*

(S//~~OC/NF~~) On July 2, 2016, the FBI interviewed Clinton. Clinton was aware she was an Original Classification Authority (OCA) at State; however, she could not recall how often she used this authority nor could she recall any training or guidance provided by State.<sup>496</sup> Clinton could not give an example of how the classification of a document was determined; rather she stated there was a process in place at State before her tenure, and she relied on career foreign service professionals to appropriately mark and handle classified information.<sup>497</sup> Clinton believed information should be classified when it relates to  the use of sensitive sources, or sensitive deliberations.<sup>498</sup> When asked whether she believed information should be classified if its unauthorized release would cause damage to national security, Clinton responded "yes, that is the understanding."<sup>499</sup>

b1  
b3

(U//~~OC/NF~~) Clinton did not recall receiving any e-mails she thought should not have been on an unclassified system.<sup>500</sup> She relied on State officials to use their judgment when e-mailing her and could not recall anyone raising concerns with her regarding the sensitivity of the information she received at her e-mail address.<sup>501</sup> The FBI provided Clinton with copies of her classified e-mails ranging from CONFIDENTIAL to TOP SECRET/SAP and Clinton said she did not believe the e-mails contained classified information.<sup>502</sup> Upon reviewing an e-mail classified SECRET//NOFORN dated December 27, 2011, Clinton stated no policy or practice existed

<sup>qqq</sup> (U//~~FOUO~~) The FBI obtained 177 of Blumenthal's memos from the e-mails provided by Williams & Connolly as part of Clinton's production to the FBI. The FBI recovered two additional memos during the investigation from BlackBerry backups provided by Cooper; State did not provide a classification determination on those additional memos.

<sup>trr</sup> (U//~~FOUO~~) According to Blumenthal, "CONFIDENTIAL" meant the memo was personal in nature and did not refer to classified USG information.

<sup>sss</sup> (U//~~FOUO~~) According to Blumenthal, the individual who provided the content for a number of the memos authored the source summary statements (caveats provided regarding the source of information) in the memos.

<sup>ttt</sup> (U//~~FOUO~~) Investigation was unable to determine if any of Blumenthal's memos were forwarded to the White House, or to other USG agencies and foreign governments, as Sullivan's OpenNet sent items were not present in the data provided by State to the FBI.

~~SECRET//ORCON/NOFORN~~ [REDACTED]

related to communicating around holidays, and it was often necessary to communicate in code or do the best you could to convey the information considering the e-mail system you were using.<sup>503</sup> In reference to the same e-mail, Clinton believed if the foreign press was to obtain information from that e-mail, it would not cause damage to the US Government.<sup>504</sup> When asked, Clinton recalled being briefed on SAP information but could not recall any specific briefing on how to handle SAP information.<sup>505</sup> Clinton stated she knew SAP information was of great importance and needed to be handled carefully.<sup>506</sup>

*F. (U//FOUO) Gaps in Clinton E-mail Recovered from Personal Server Systems*

(U//FOUO) There were no e-mails provided by Williams & Connolly to State or the FBI dated from January 21, 2009 to March 18, 2009. FBI investigation identified an additional 18 days where Clinton did not provide State any responsive e-mail. FBI investigation determined 14 of the 18 days where Clinton did not provide State any responsive e-mail correspond with e-mail outages affecting Clinton's personal server systems as a result of both Hurricane Irene<sup>uuu</sup> and Hurricane Sandy<sup>vvv</sup>. FBI investigation indicated other explanations for gaps in Clinton's e-mail production could include user deletion prior to PRN's transfer of Clinton's e-mails for review, or flaws in the archiving and sorting process used to generate the responsive production to State.

**4. (U//FOUO) Results of the FBI Investigation and Analysis of Cyber Intrusion Potential**

*A. (U//FOUO) Cyber Analysis of Clinton's Personal Server Systems*

(U//FOUO) FBI investigation and forensic analysis did not find evidence confirming that Clinton's e-mail server systems were compromised by cyber means. The FBI's inability to recover all server equipment and the lack of complete server log data for the relevant time period limited the FBI's forensic analysis of the server systems. As a result, FBI cyber analysis relied, in large part, on witness statements, e-mail correspondence, and related forensic content found on other devices to understand the setup, maintenance, administration, and security of the server systems.

(U//FOUO) Investigation determined Clinton's clintonemail.com e-mail traffic was potentially vulnerable to compromise when she first began using her personal account in January 2009. It was not until late March 2009, when the Pagliano Server was set up and an SSL certificate<sup>www</sup> was acquired for the clintonemail.com domain—providing encryption of login credentials, but not e-mail content stored on the server—that access to the server was afforded an added layer of security.<sup>507,508</sup> The certificate was valid until September 13, 2013, at which time PRN obtained a new certificate valid until September 13, 2018.<sup>509</sup>

(U//FOUO) During his December 22, 2015 FBI interview, Pagliano recalled a conversation with [REDACTED] at the beginning of Clinton's tenure, in which [REDACTED] advised he would not be

b6  
b7C

<sup>uuu</sup> (U//FOUO) The first of two extended outages occurred from August 28 to 30, 2011 (3 days) as a result of Hurricane Irene.

<sup>vvv</sup> (U//FOUO) The second extended outage occurred from October 30, 2012 to November 9, 2012 (11 days) as a result of Hurricane Sandy.

<sup>www</sup> (U//FOUO) According to FBI forensic analysis, there was no SSL certificate on the Pagliano Server between March 19, 2009, when the mail service was operational, and March 29 or 30, 2009, when the SSL certificate was installed on the server.

~~SECRET//ORCON/NOFORN~~ [REDACTED]

~~SECRET//ORCON/NOFORN~~ [REDACTED]

surprised if classified information was being transmitted to Clinton's personal server.<sup>510</sup>

[REDACTED] further recommended that e-mail transiting from a state.gov account to the server should be sent through a Transport Layer Security (TLS)<sup>xxx</sup> tunnel.<sup>yyy</sup> Pagliano advised that the transition to TLS never occurred.<sup>511,512</sup> The FBI was unable to forensically determine if TLS was implemented on the Pagliano Server.

b6  
b7C

(U//~~FOUO~~) When asked about the maintenance and security of the server system he administered, Pagliano stated there were no security breaches, but he was aware there were many failed login attempts, which he referred to as brute force attacks.<sup>zzz,513</sup> He added that the failed attempts increased over the life of the Pagliano Server, and he set up the server's logs to alert Cooper when they occurred.<sup>514</sup> Pagliano knew the attempts were potential attackers because the credentials attempting to log in did not match legitimate users on the system.<sup>515</sup> Pagliano could not recall if a high volume of failed login attempts emanated from any specific country.<sup>516</sup>

(U//~~FOUO~~) In an attempt to thwart potential attacks, Pagliano set up Internet Protocol (IP) filtering<sup>aaaa</sup> on the firewall and tried to review the firewall log files once a month.<sup>517</sup> After the Pagliano Server was established, Cooper put Pagliano in contact with [REDACTED] a United States Secret Service (USSS) agent, who recommended Pagliano also perform outbound filtering of e-mail traffic.<sup>518</sup> Pagliano further considered, but ultimately did not implement, a Virtual Private Network (VPN)<sup>bbbb</sup> or two-factor authentication<sup>cccc</sup> to better secure administrative access to the server system by him and Cooper.<sup>519</sup> The FBI forensically determined that Remote Desktop Protocol (RDP)<sup>dddd</sup> was enabled on the Pagliano Server and was used by Pagliano, Cooper, and later PRN, for remote administration of the server.<sup>520</sup> While the availability of RDP

b6  
b7C

---

<sup>xxx</sup> (U) TLS is a protocol that ensures privacy between communicating applications, such as web browsing, e-mail, and instant-messaging, with their users on the Internet. TLS ensures that no third-party eavesdrops on the two-way communication. TLS is the successor to SSL and is considered more secure.

<sup>yyy</sup> (U) According to the State OIG report, State policy (12 FAM 544.3) stipulates normal day-to-day operations must be conducted on an authorized system. In the absence of a device, such as a State OpenNet terminal, employees can send most Sensitive But Unclassified (SBU) information unencrypted via the Internet only when necessary, with the knowledge that the nature of the transmission lends itself to unauthorized access, however remote that chance might be. Furthermore, in August 2008, 12 FAM 682.2-5 was amended and mandated that SBU information on non-Department-owned systems at non-Departmental facilities had to meet certain criteria. Employees had to: 1) ensure that SBU information was encrypted; 2) destroy SBU information on their personally owned and managed computers and removable media when the files are no longer required; and 3) implement encryption certified by the National Institute of Science and Technology (NIST), among other things. Although 12 FAM 682.2-5 was further amended in 2009, 2011, 2014, and 2015, the basic requirements did not change.

<sup>zzz</sup> (U) A brute force attack is a trial-and-error method used to obtain information, such as a password or personal identification number (PIN). In a brute force attack, passwords may be attempted manually or automated software can be used to generate a large number of consecutive guesses as to the targeted information.

<sup>aaaa</sup> (U) IP filtering is the practice of identifying and manually blocking IP addresses based on the identification of patterns that are indicative of a potential attack.

<sup>bbbb</sup> (U) VPN is a private network that runs on top of a larger network to provide access to shared network resources, which may or may not include the physical hard drives of individual computers, as in the case of Remote Desktop Protocol (RDP). VPN offers an additional layer of security by encrypting the data traveling to the private network before sending it over the Internet. Data is then decrypted when it reaches the private network.

<sup>cccc</sup> (U) Two-factor authentication is a method of confirming a user's claimed identity by utilizing a combination of two different components, often something the user knows and something the user has—such as a RSA keyfob/token.

<sup>dddd</sup> (U) RDP is a proprietary protocol developed by Microsoft that allows a user to remotely connect to another computer over a network connection to view the computer and control it remotely. RDP is implemented in every version of Windows starting with Windows XP.

~~SECRET//ORCON/NOFORN~~ [REDACTED]

on a server is convenient for remote access, the FBI is aware of known vulnerabilities<sup>eeee</sup> associated with the protocol.

(U//~~FOUO~~)

b3

<sup>523, 524</sup> Pagliano recalled finding “a virus,” but could provide no additional details, other than it was nothing of great concern.<sup>525</sup> FBI examination of the Pagliano Server and available server backups did not reveal any indications of malware.<sup>526</sup>

(U//~~FOUO~~) On January 9, 2011, Cooper sent Abedin an e-mail stating someone was attempting to “hack” the server, prompting him to shut it down.<sup>527</sup> Cooper sent Abedin another e-mail later the same day stating he had to reboot the server again.<sup>528</sup> The FBI's investigation did not identify successful malicious login activity associated with this incident.<sup>529</sup>

(U//~~FOUO~~) The FBI's review of available Internet Information Services (IIS) web logs showed scanning attempts from external IP addresses over the course of Pagliano's administration of the server, though only one appears to have resulted in a successful compromise of an e-mail account on the server.<sup>530</sup> Forensic analysis noted that on January 5, 2013, three IP addresses matching known Tor<sup>ffff</sup> exit nodes were observed accessing a user e-mail account on the Pagliano Server believed to belong to President Clinton staffer  FBI investigation indicated the Tor user logged in to  e-mail account and browsed e-mail folders and attachments.<sup>531, 532</sup> When asked during her interview,  stated to the FBI she is not familiar with nor has she ever used Tor software.<sup>533</sup> FBI investigation to date was unable to identify the actor(s) responsible for this login or how  login credentials were compromised.<sup>534</sup>

b6  
b7C

(U//~~FOUO~~) Forensic analysis of alert e-mail records automatically generated by CloudJacket revealed multiple instances of potential malicious actors attempting to exploit vulnerabilities on the PRN Server. FBI determined none of the activity, however, was successful against the server.<sup>535</sup>

(U//~~FOUO~~) Following the March 3, 2015 *New York Times* article publicly revealing Clinton's use of personal e-mail to conduct government business,<sup>536</sup> the FBI identified an increased number of login attempts to the PRN Server and its associated domain controller.<sup>gggg, 537</sup> Forensic analysis revealed none of the login attempts were successful. FBI investigation also identified an

---

<sup>eeee</sup> (U) Older versions of RDP had a vulnerability in the method used to encrypt RDP sessions. While security patches, if applied, have remedied these vulnerabilities, exposing RDP to direct connections could allow remote attackers the opportunity to guess login credentials.

<sup>ffff</sup> (U) Tor is free software allowing end users to direct their Internet traffic through a group of volunteer-operated servers around the world in order to conceal their location and Internet usage.

<sup>gggg</sup> (U) A domain controller is a Microsoft server that responds to security authentication requests (logins, checking permissions, etc.) within a Windows domain.

increase in unauthorized login attempts into the Apple iCloud<sup>hhhh</sup> account likely associated with Clinton's e-mail address<sup>iiii</sup> during this time period. Investigation determined all potentially suspicious Apple iCloud login attempts were unsuccessful.<sup>538</sup> Additionally, PRN made various network changes to the PRN Server around March 7, 2015, to include disabling the server's public-facing VPN page and switching from SSL protocol to TLS to increase security.<sup>539</sup> Staff also discussed the possibility of conducting penetration testing<sup>iii</sup> against the PRN Server to highlight vulnerabilities in the network.<sup>540</sup> The FBI interviewed an employee of the company with which PRN had discussed the issue. The employee stated that the topic was broached but that penetration testing against the PRN Server, ultimately, did not happen.<sup>541</sup>

*B. (U//~~FOUO~~) Cyber Analysis of Clinton's Mobile Devices*

(U//~~FOUO~~) The FBI does not have in its possession any of Clinton's 13 mobile devices which potentially were used to send e-mails using Clinton's clintonemail.com e-mail addresses. As a result, the FBI could not make a determination as to whether any of the devices were subject to compromise. Similarly, the FBI does not have in its possession two of the five iPad devices which potentially were used by Clinton to send and receive e-mails during her tenure.<sup>542,543,544,545</sup> The FBI forensically examined two of the three iPads<sup>kkkk</sup> it obtained and found no evidence of cyber intrusion.<sup>546</sup>

*C. (U//~~FOUO~~) Cyber Targeting of Clinton's Personal E-mail and Associated Accounts*

(S//~~OC/NF~~) Investigation identified multiple occurrences of phishing and/or spear-phishing e-mails sent to Clinton's account during her tenure as Secretary of State.<sup>547</sup> [redacted]

b1  
b3  
b6  
b7C

(S//~~OC/NF~~) Clinton received another phishing e-mail, purportedly sent from the personal e-mail account of a State official [redacted]. The e-mail contained a potentially malicious link.<sup>552</sup> Clinton replied to the e-mail [redacted] stating, "Is this really from you? I was worried about opening it!"<sup>553</sup> [redacted]  
In a separate incident [redacted] Abedin sent an e-mail to [redacted] indicating Clinton was

b1  
b3  
b6  
b7C

<sup>hhhh</sup> (U//~~FOUO~~) Apple iCloud is a cloud storage medium available to users of Apple products. Clinton is known to have used Apple iPads during the course of her tenure, and hdr22@clintonemail.com was likely used as her AppleID to set up a new Apple device.

<sup>iiii</sup> (U//~~FOUO~~) While the NYT article did not reveal Clinton's e-mail address—and by default the domain name—it is very likely those who tried to gain access to the related Apple iCloud account searched for and found the e-mail address in open sources. News articles from 2013 contained a screenshot of Blumenthal's communication with "hdr22," thereby divulging Clinton's e-mail alias. Other outlets mentioned the domain name in articles but withheld Clinton's e-mail alias. Clinton's full e-mail address could therefore have been ascertained through piecing together various sources.

<sup>iii</sup> (U) Penetration testing, more commonly known as pentesting, is the practice of testing a computer system, network, or web application to find vulnerabilities that an attacker could exploit.

<sup>kkkk</sup> (U//~~FOUO~~) The third iPad the FBI obtained was not actually used by Clinton. Shortly after it was purchased, it was given as a gift to a member of her staff, and therefore the FBI did not forensically examine the device.

<sup>llll</sup> (U) RAT is a piece of software that facilitates remote operation of a computer system.

worried “someone [was] hacking into her email” given that she received an e-mail from a known [redacted] associate containing a link to a website with pornographic material.<sup>554</sup> There is no additional information as to why Clinton was concerned about someone hacking into her e-mail account, or if the specific link referenced by Abedin was used as a vector to infect Clinton's device [redacted]

b6  
b7C

(S) [redacted] Open source information indicated, if opened, the targeted user's device may have been infected, and information would have been sent to at least three computers overseas, including one in Russia.<sup>560,561</sup> [redacted]  
[redacted]

b1  
b3

D. (U//~~FOUO~~) Potential Loss of Classified Information

(U//~~FOUO~~) On March 11, 2011, Boswell sent a memo directly to Clinton outlining an increase since January 2011 of cyber actors targeting State employees' personal e-mail accounts.<sup>563</sup> The memo included an attachment which urged State employees to limit the use of personal e-mail for official business since “some compromised home systems have been reconfigured by these actors to automatically forward copies of all composed e-mails to an undisclosed recipient.”<sup>564</sup> Clinton's immediate staff was also briefed on cybersecurity threats in April and May 2011.<sup>565</sup>

(S//~~OC/NF~~) [redacted]  
[redacted]b1  
b3  
b6  
b7C  
b7E(S//~~OC/NF~~) [redacted]  
[redacted]b1  
b3  
b6  
b7C  
b7E

<sup>nnnnn</sup> (U) In order for malicious executables to be effective, the targeted host device has to have the correct program/applications installed. If, for example, the host is running an older version of Adobe but the exploit being used is newer, there is a chance the host will not be infected because the exploit was unable to execute using the older version of the program.

<sup>nnnn</sup> (U) A “drop” account, in this case, is an e-mail account controlled by foreign cyber actors and which serves as the recipient of auto-forwarded e-mails from victim accounts.

(U//~~FOUO~~) On or about March 14, 2013, Blumenthal's AOL e-mail account was compromised by Marcel Lehel Lazar, aka Guccifer, a Romanian cyber hacker. Lazar disseminated e-mails and attachments sent between Blumenthal and Clinton to 31 media outlets, including a Russian broadcasting company.<sup>587</sup> [redacted]

b7E

[redacted]<sup>588</sup> One of the screenshots captured a list of 19 foreign policy and intelligence memos authored by Blumenthal for Clinton.<sup>589</sup> The content of one of the memos on the list was determined by State to be classified at the CONFIDENTIAL level.<sup>590</sup> Lazar was extradited from Romania to the United States on March 31, 2016.<sup>591</sup>

(U//~~FOUO~~) Between April 25, 2016 and May 2, 2016, Lazar made a claim to FOX News that he used information from Blumenthal's compromise as a stepping stone to hack Clinton's personal server.<sup>592</sup> On May 26, 2016, the FBI interviewed Lazar, who admitted he lied to FOX News about hacking the Clinton server.<sup>593</sup> FBI forensic analysis of the Clinton server during the timeframe Lazar claimed to have compromised the server did not identify evidence that Lazar hacked the server.<sup>594</sup> An examination of log files from March 2013 indicated that IP addresses from Russia and Ukraine attempted to scan the server on March 15, 2013, the day after the Blumenthal compromise, and on March 19 and March 21, 2013.<sup>595</sup> However, none of these attempts were successful, and it could not be determined whether this activity was attributable to Lazar.<sup>596</sup>

E. (U//~~FOUO~~) General Cyber Analysis Conducted

(S//~~OC/NF~~) [redacted] The FBI conducted general cyber research and analysis of e-mail addresses and user accounts associated with the clintonemail.com and presidentclinton.com domains.

b1  
b3  
b6  
b7C  
b7E

(U//~~FOUO~~) FBI extracted the Thread-Index<sup>oooo</sup> and Message-ID<sup>pppp</sup> values for each identified confirmed classified e-mail relevant to this investigation. The values were extracted from the e-mail headers<sup>qqqq</sup> in order to develop specific electronic signatures that could be used when searching for exact references in large data repositories. In an effort to identify whether any confirmed classified e-mails may have been compromised through computer intrusion methods, the FBI conducted signature-based searches in available databases, to include [redacted]<sup>rrr</sup>. The FBI also provided the unique identifiers to other government agencies, and one entity

b7E

<sup>oooo</sup> (U) A Thread-Index value is a unique, alphanumeric, Microsoft Outlook-centric field found in an e-mail's header. The identifier is used to track e-mail threads (or conversations). Each time there is a reply or forward in the e-mail thread, Outlook—if it is the e-mail client being used—will append additional alphanumeric characters to the e-mail's original Thread-Index value.

<sup>pppp</sup> (U) A Message-ID is a unique identifier found in an e-mail's header. Message-IDs are required to have a specific format and be globally unique. Unlike Thread-Index values, Message-IDs are unique to every individual e-mail, regardless of whether two e-mails belong to the same thread (or conversation).

<sup>qqqq</sup> (U) A header precedes the body (content text) of an e-mail, and contains lines (metadata) that identify particular routing information. Fields such as "From," "To," and "Date" are mandatory, while others are optional.

<sup>rrr</sup> (U//~~FOUO~~) [redacted]

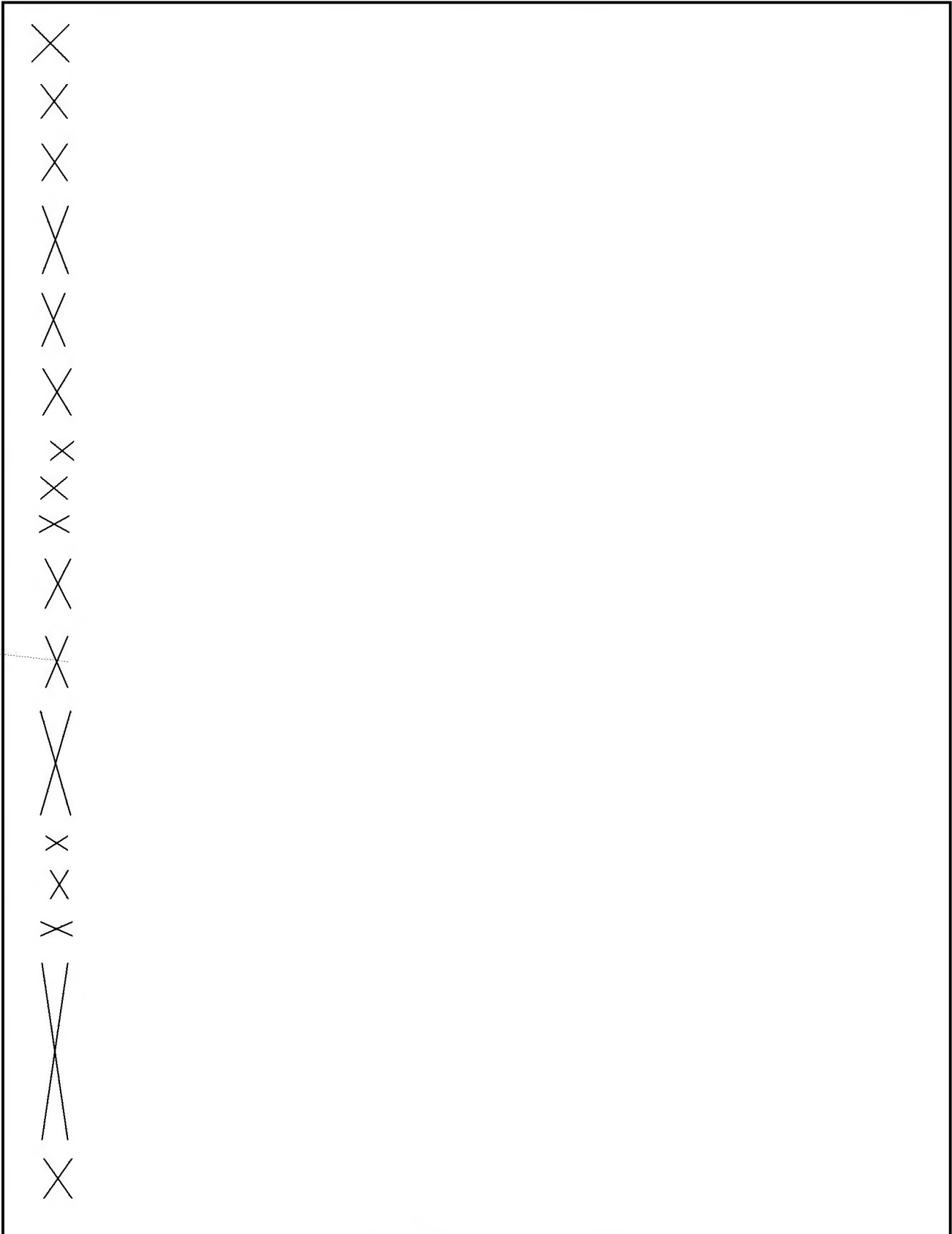
b7E



responded.<sup>ssss</sup> To date, the signature-based searches in USG databases have not identified the relevant e-mails.<sup>601</sup>

---

<sup>ssss</sup> (U//~~FOUO~~) The FBI provided the Executive Office of the President (EOP), State Cyber Threat Analysis Division (CTAD), and State's Information Resource Bureau (IRB) with Thread-Index and Message-ID values. CTAD found no record of the signatures provided. EOP stated they could only search "To," "From," and "Subject" lines, as did State IRB. Separately, in an attempt to identify whether confirmed classified e-mails resided in unidentified e-mail provider accounts, or whether identified accounts forwarded or replied to the classified messages, the FBI explored the possibility of sharing Thread-Index Value and Message-IDs with e-mail service providers of interest. Google was asked if they could search those header fields in its dataset. The company stated it does not index Thread-Index values, which is the identifier the FBI was most interested in, as it would have provided insight into the extent the messages were forwarded.

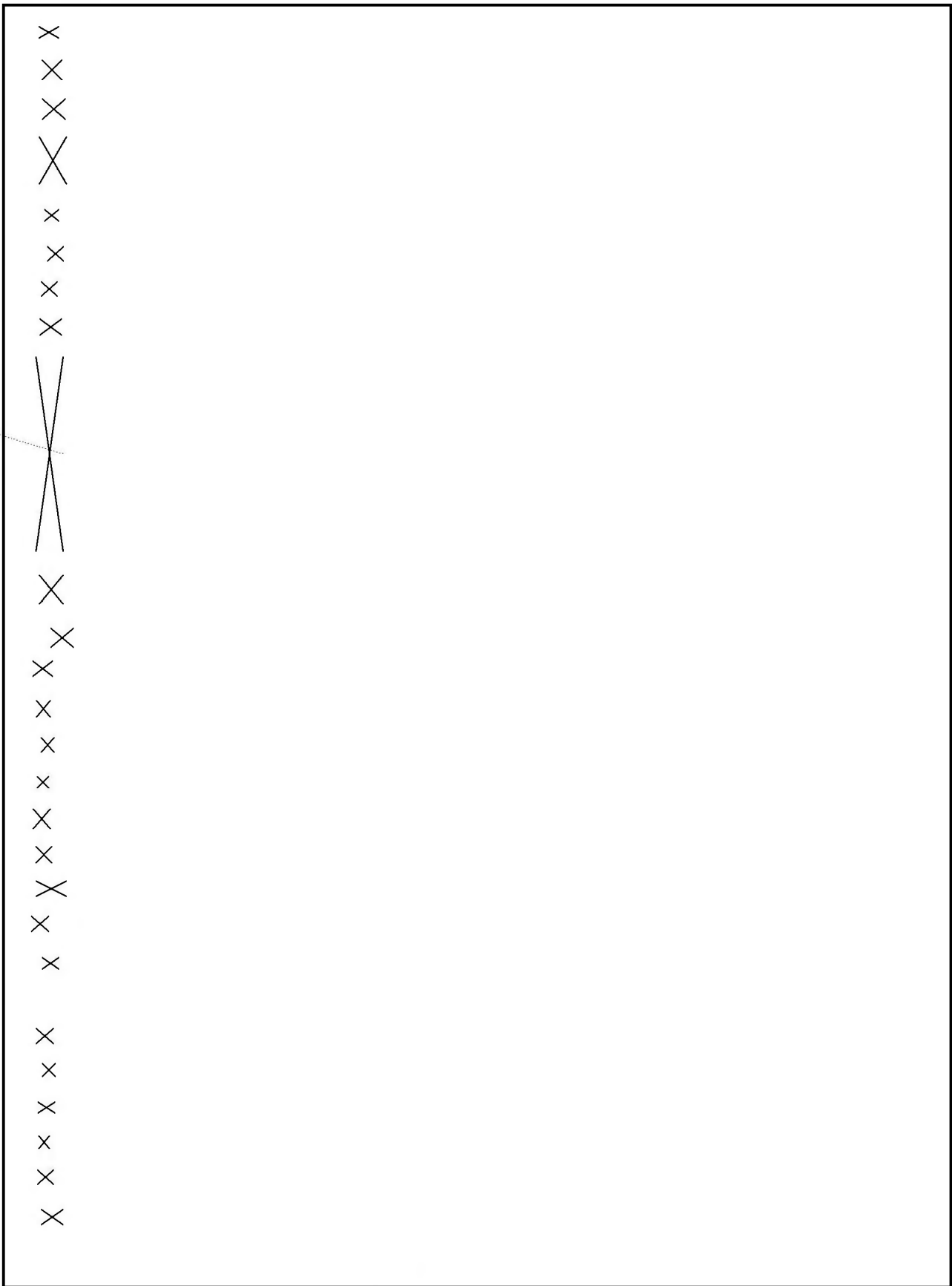


b3  
b5  
b6  
b7C  
b7E

~~SECRET//ORCON/NOFORN~~

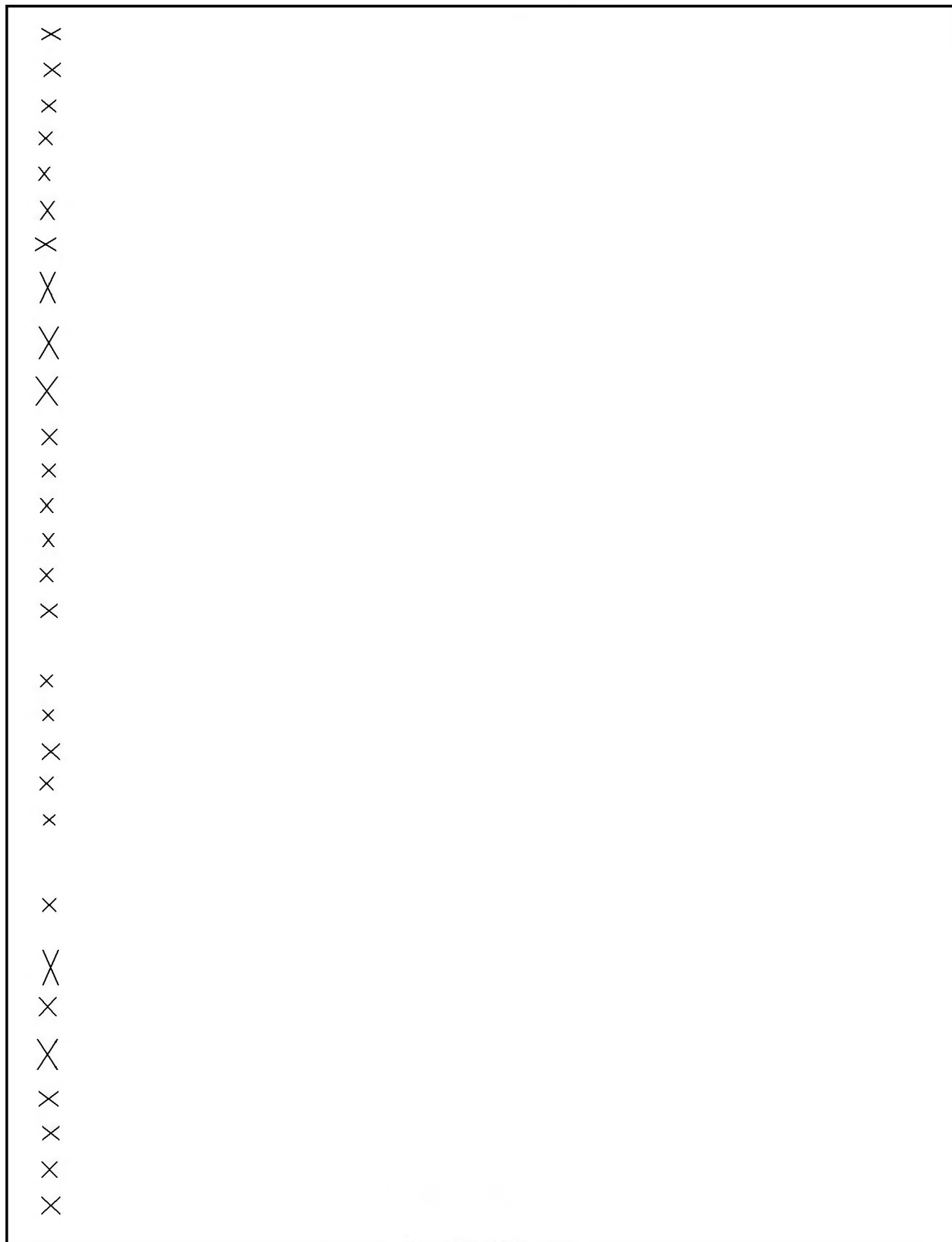
(U)

b3  
b5  
b6  
b7C  
b7E



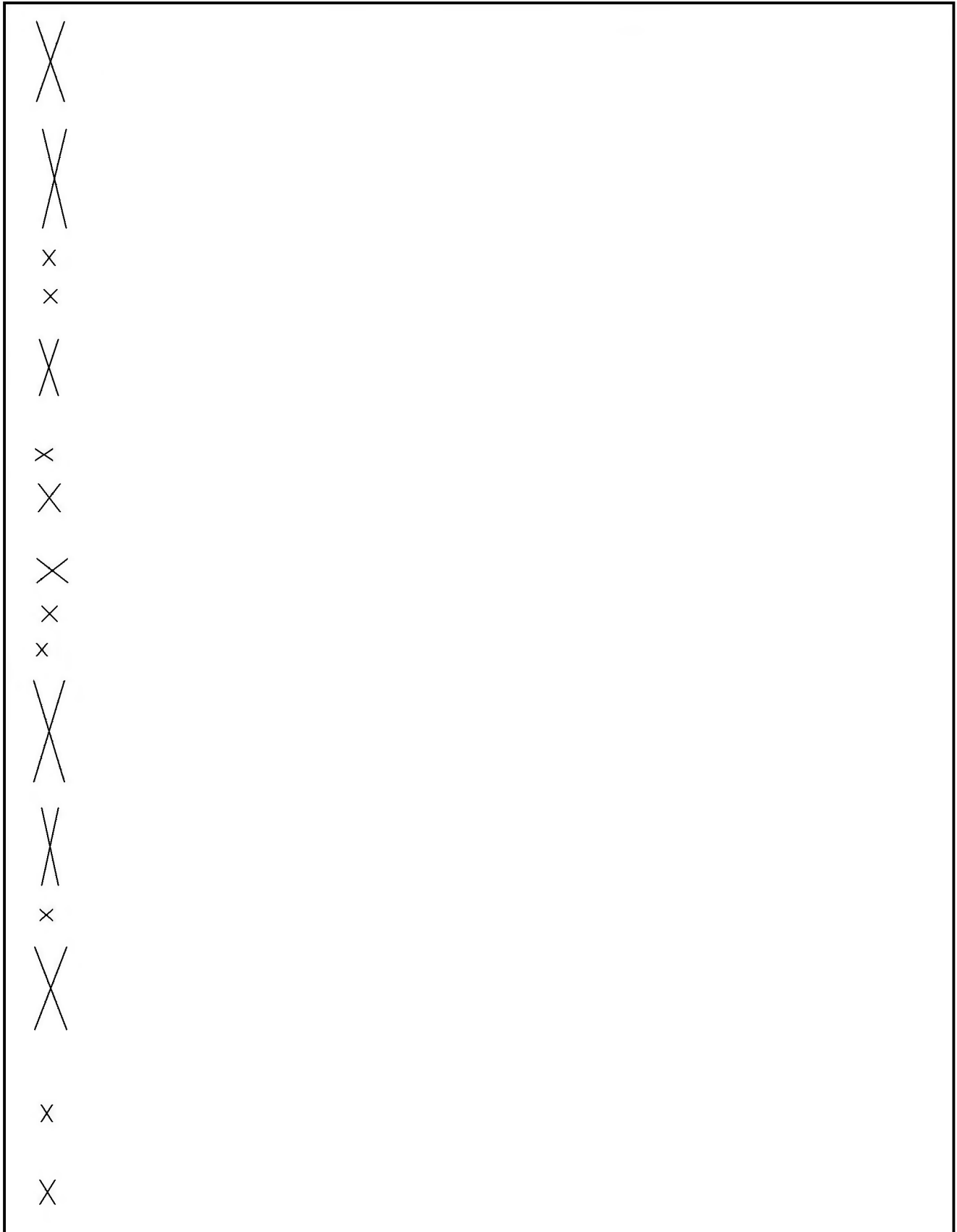
~~SECRET//ORCON/NOFORN~~

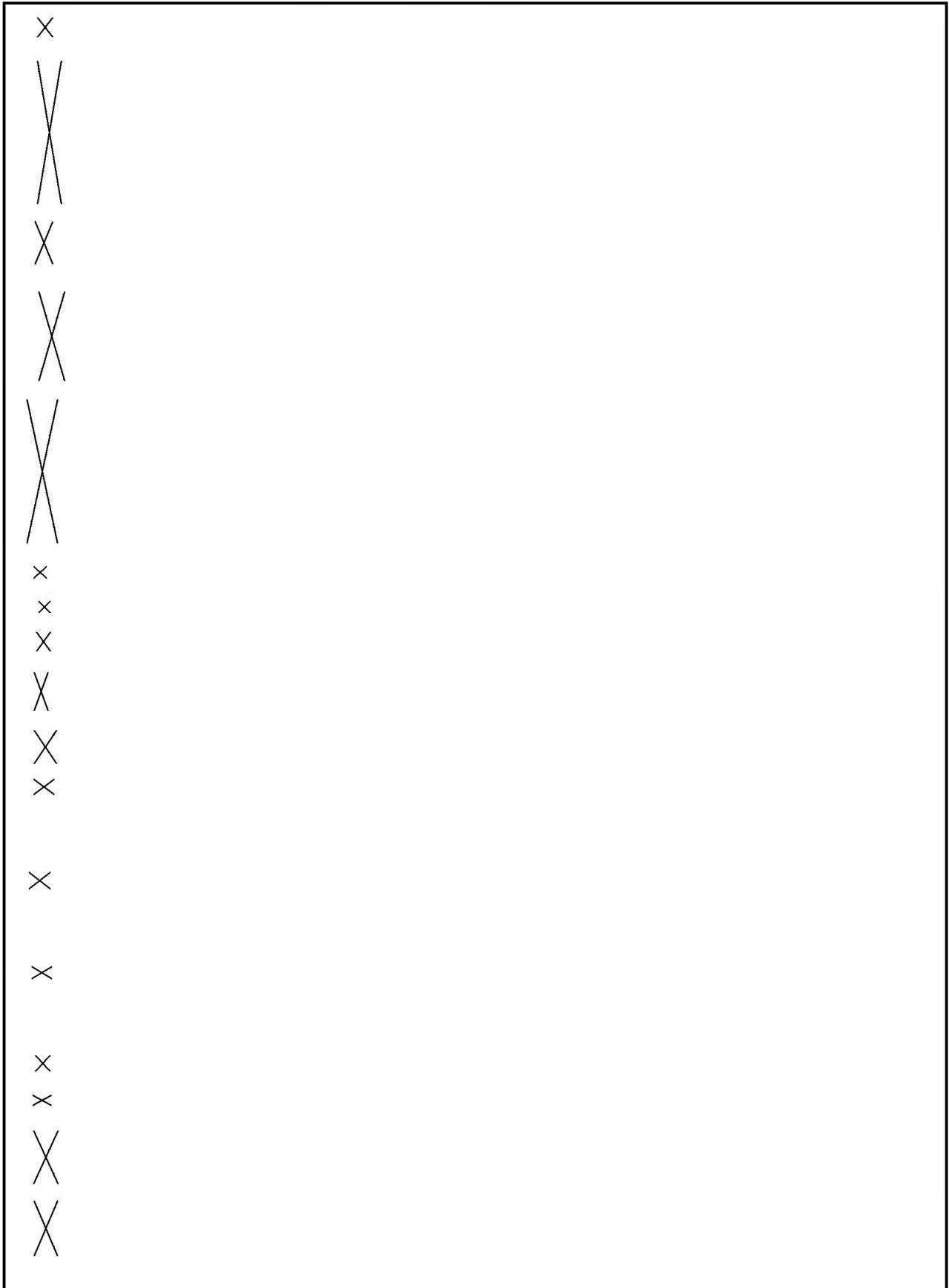
b1  
b3  
b7E

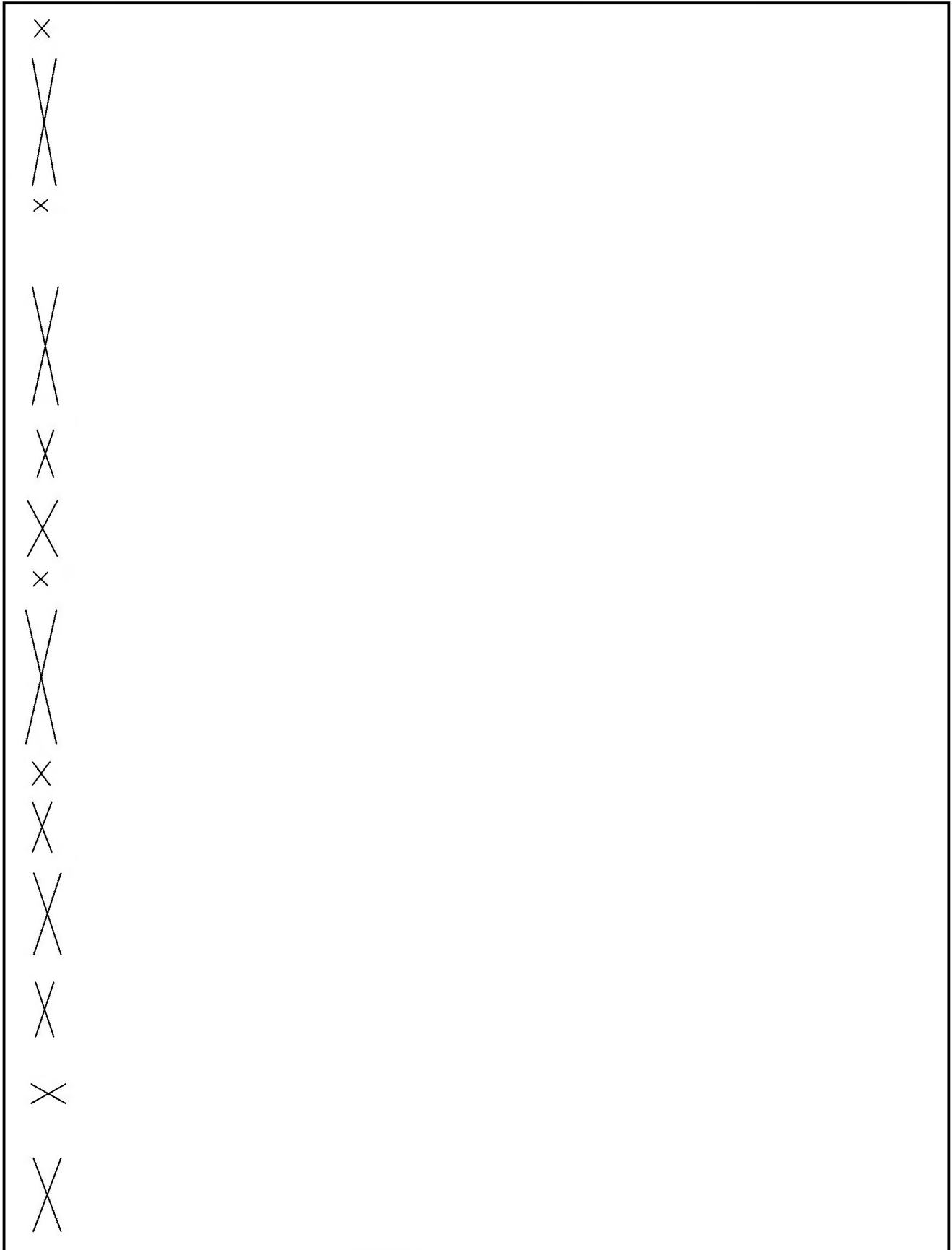


b1  
b3  
b5  
b6  
b7C  
b7E

b1  
b3  
b7E











b1  
b3  
b7E

(U)

×

×

×

×

×

×

b3  
b5  
b6  
b7C  
b7E



b1  
b3  
b7E

b3  
b5  
b6  
b7C  
b7E

(C)

\_\_\_\_\_

b1  
b3  
b7E

**b1**

b3

b7E

X

X

V

X

 $\wedge$ 

Y

/ /

✓

✓

X

X

 $\vee$  $\wedge$ 

X

X

X

X

V

 $\wedge$ 

~~X~~

V

 $\Delta$ 

V

 $\Delta$ 

X

X

✓

1

✓

b3

b5

b6

b7c

b7E

b1

b3

b7E

(U)

b3  
b5  
b7E

b1  
b3  
b7E



b1  
b3  
b7E

(U)

X

X

x

X

X

x

X

X

X

X

X

X

X

X

X

X

X

x

x

X

x

X

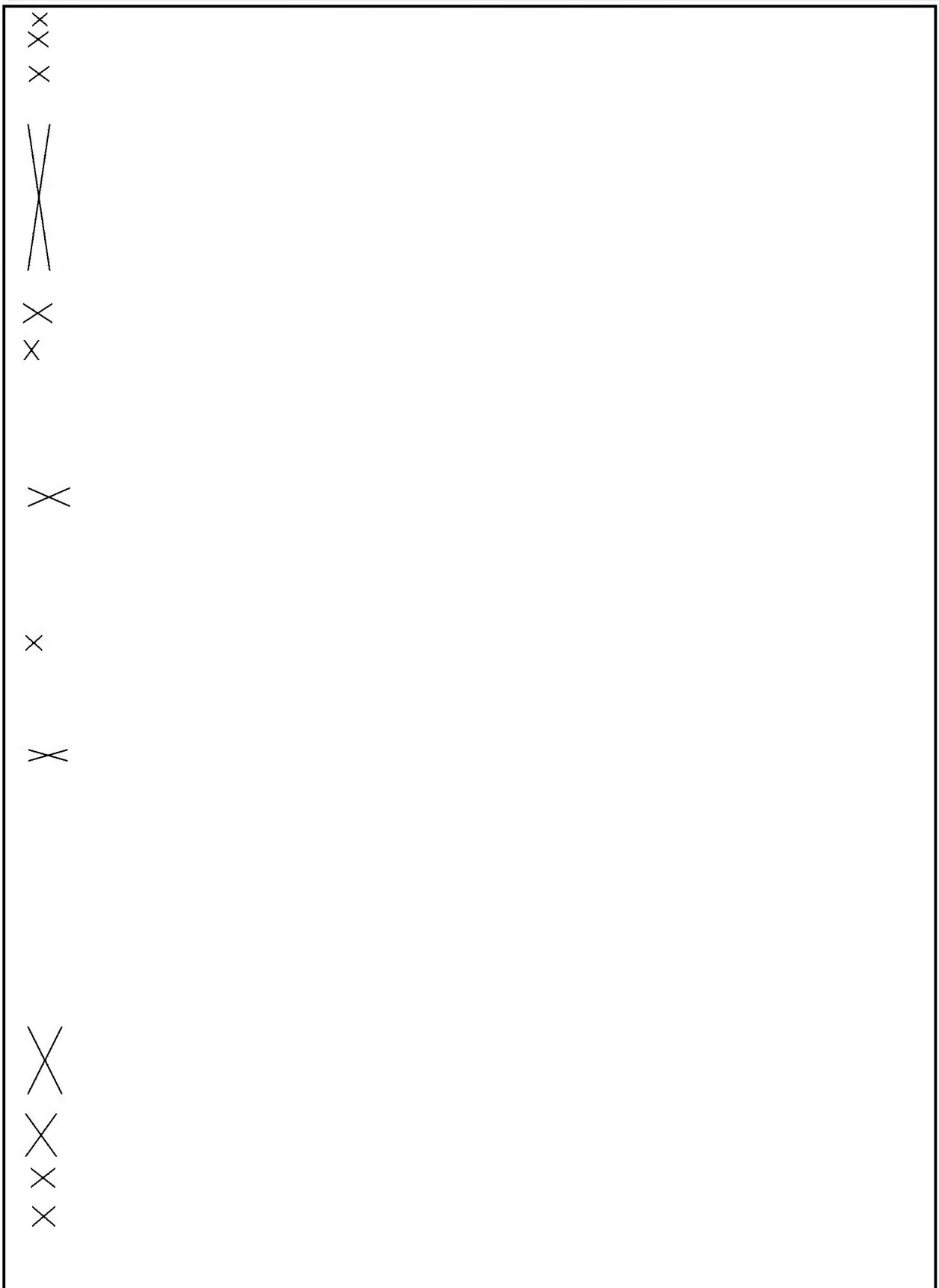
X

b3  
b5  
b6  
b7C  
b7E



b1  
b3  
b7E

b1  
b3  
b7E



b1  
b3  
b5  
b6  
b7C  
b7E

b1  
b3  
b7E



×	
×	
×	
×	
×	
×	
×	
×	

~~TOP SECRET~~

~~/OC/NF~~

b1  
b3

FD-302a (Rev. 10-6-95)

-I-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/02/2016

(U//~~FOUO~~) On July 2, 2016, HILLARY RODHAM CLINTON, date of birth [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED] at the J. Edgar Hoover Building located at 935 Pennsylvania Avenue NW, Washington, DC 20535. Present for the interview were CLINTON's attorneys David E. Kendall, Katherine M. Turner, Cheryl D. Mills, Heather Samuelson and [REDACTED]. Also present was FBI Section Chief Peter P. Strzok, as well as David Laufman, [REDACTED] and [REDACTED] from the Department of Justice (DOJ). Prior to the interview, Kendall, Turner, [REDACTED] and Samuelson agreed to sign a non-disclosure agreement in anticipation of viewing documents during the interview that were classified as part of a Special Access Program (SAP). After being advised of the identities of the interviewing agents, and the purpose of the interview, CLINTON provided the following information:

b6  
b7C

(U//~~FOUO~~) Upon taking office as the Secretary of State (SecState) at the U.S. Department of State (hereafter, State) in January 2009, CLINTON recalled her office on the seventh floor at State headquarters had one black phone capable of unsecure and secure communications, one yellow phone for secure communication only, and one white phone capable of direct calls to certain government officials. CLINTON did not have a computer terminal of any kind or a facsimile machine in her office at State. Additionally, State outfitted CLINTON's residences in Washington, DC and Chappaqua, New York with a Sensitive Compartmented Information Facility (SCIF). Each SCIF had a combination lock that only CLINTON knew the combination to. The SCIFs in both residences were outfitted with secure video teleconference equipment, and the same phone systems as in her office at State. CLINTON did not have a computer terminal of any kind in the SCIFs at her residences, but did have a facsimile machine capable of secure and unsecure transmission. CLINTON rarely used the SCIF in her residence in DC, primarily due to her preference to use her office at State. It was CLINTON's practice to lock the SCIF every time it was vacated. When in her residences, CLINTON would receive classified information through diplomatic pouch via courier, secure phone call or secure fax. After consuming hard copy classified documents at her residence, CLINTON would place the documents in a "burn bag."

(S//~~NF~~) When traveling domestically, CLINTON had no technical support traveling with her as it related to secure communications. [REDACTED] CLINTON recalled verbal briefings on the security of her communications [REDACTED]. For instance, CLINTON [REDACTED]

b1  
b3

Investigation on 07/02/2016 at Washington DC

File # [REDACTED] Date dictated N/A

b3  
b7E

By SA [REDACTED] SA [REDACTED]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~

~~/OC/NF~~

b1  
b3

~~TOP SECRET~~~~#OC/NF~~b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 2

[REDACTED] CLINTON stated that Diplomatic Security would handle communication infrastructure in certain instances [REDACTED] in which classified information could be communicated.

b1  
b3

(S//NF)

(U//~~FOUO~~) After reviewing an email dated July 1, 2012 with subject line "Fw: Congratulations!," CLINTON stated she received no particular guidance as to how she should use the President's email address [REDACTED]@who.eop.gov. Since the foregoing email was sent from Russia, CLINTON stated she must have sent it from the plane.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated March 22, 2009 with subject line "Re: Follow up," CLINTON stated this email pertained to how her "files" were going to be treated at State. CLINTON relayed while in the Senate, she maintained a personal and official paper file. This process was not implemented through Senate procedure or guidance but through CLINTON's own personal process. CLINTON was not aware how other State staff maintained their records and was unaware of State's State Messaging and Archive Retrieval Toolset (SMART).

(U//~~FOUO~~) CLINTON could not recall when she first received her security clearance and if she carried it with her to State via reciprocity from her time in the Senate. CLINTON could not recall any briefing or training by State related to the retention of federal records or handling of classified information.

(U//~~FOUO~~) CLINTON was aware she was an Original Classification Authority (OCA) at State. CLINTON could not recall how often she used this authority or any training or guidance provided by State. CLINTON could not give an example of how classification of a document was determined. CLINTON stated there was a process at State before she arrived and she relied on the career foreign service professionals she worked with to appropriately handle and mark classified information.

(U//~~FOUO~~) CLINTON recalled being briefed on Special Access Program (SAP) information but could not recall any specific briefing on how to handle information associated with SAPs. CLINTON was certain she signed an agreement memorializing her access to SAP material, but she could not recall specific detail. CLINTON recalled all SAP related information was delivered to her by paper in her office, through courier at her residence, or through conversation in her office or in the Situation Room at the White House. In general, CLINTON knew SAP information was of great importance and needed to be handled carefully.

~~TOP SECRET~~~~#OC/NF~~b1  
b3

~~TOP SECRET~~~~/OC/NF~~b1  
b3Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 3b1  
b3

[REDACTED] CLINTON could not recall a specific process for nominating a target for a drone strike and recalled much debate pertaining to the concurrence process. CLINTON knew there was a role for DOD, State and the CIA but could not provide specifics as to what it was. Due to a disagreement between these agencies, CLINTON recalled having many discussions related to nominating an individual for a drone strike. [REDACTED]

b1  
b3

[REDACTED]

When CLINTON exchanged classified information pertaining to the drone program internally at State, it was in her office or on a secure call. When CLINTON exchanged classified information pertaining to the drone program externally it was at the White House. CLINTON never had a concern with how classified information pertaining to the drone program was handled.

(U//~~FOUO~~) CLINTON was not issued a mobile device by State, but continued to use the password protected BlackBerry she used during her time in the Senate. This device was connected to her AT&T BlackBerry address which was used for both personal communications and official business. CLINTON made this decision out of convenience and noted she had spoken to former Secretary of State COLIN POWELL who used a private email account, as had other Secretaries of State before him.

(U//~~FOUO~~) After reviewing an email dated February 12, 2009 with the subject line "Re: New cell," CLINTON stated she was familiar with the phone number ending in [REDACTED] referenced in the email. She believed the number was that of her BlackBerry because she did not recall using a flip phone during her time at State, only while in the Senate.

b6  
b7C

(U//~~FOUO~~) When CLINTON's BlackBerry device malfunctioned, her aides would assist in obtaining a new BlackBerry. After moving to the new device, her old SIM card was disposed of by her aides. CLINTON did not recall how any data stored on the device was destroyed. CLINTON's aides would also assist in setting up the new BlackBerry and implementing any security features.

(U//~~FOUO~~) While on international travel, CLINTON never suspected her BlackBerry was tampered with, nor did she ever lose a BlackBerry while traveling. There were a few occasions where

~~TOP SECRET~~~~/OC/NF~~b1  
b3

~~TOP SECRET~~~~SECRET~~b1  
b3Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 4

CLINTON's staff was provided with a secure cell phone, but CLINTON did not recall the circumstances or frequency with which this event occurred.

(U//~~FOUO~~) CLINTON requested a secure BlackBerry while at State, but could not recall why they were unable to provide one. She was aware President Obama had one and it seemed convenient. Her request was not out of concern for the sensitivity of the information on her then-current device. CLINTON wanted the secure BlackBerry to deal with any future contingencies and thought it would be a good idea to have a secure cell. After reviewing a memo written for CHERYL MILLS by ERIC BOSWELL, CLINTON stated she never brought her unclassified BlackBerry into her SCIF for the reasons outlined in the memo. She would keep her BlackBerry outside of the SCIF and check it in non-SCIF areas of State, when traveling to her office, at speeches, and other occasions outside of the office.

(U//~~FOUO~~) CLINTON did not recall receiving any emails she thought should not be on an unclassified system. She relied on State officials to use their judgment when emailing her and could not recall anyone raising concerns with her regarding the sensitivity of the information she received at her email address. CLINTON had frequent in-person meetings with State personnel where classified information was communicated, including a daily 8:30 AM staff meeting and numerous other walk-in and walk-out meetings during the day.

(U//~~FOUO~~) CLINTON used a private email address with AT&T during her time in the Senate for official and personal use. CLINTON recalled knowing her husband, WILLIAM J. CLINTON, had private email addresses for his aides. CLINTON did not recall her specific conversations regarding the creation of the clintonemail.com domain, but around January 2009, directed aides to create the email account. It was a matter of convenience to move onto a system maintained by her husband's staff. CLINTON was aware there was a server in her basement at Chappaqua, but did not know of the various server systems until being made aware recently. CLINTON did not recall receiving guidance from State regarding email policies outlined in the Foreign Affairs Manual. CLINTON advised everyone at State knew she had a private email address because it was displayed to anyone with whom she exchanged emails; however, she did not explicitly request permission to use a private server or email address. During her tenure, no one at State raised concerns regarding CLINTON's use of a private server or email address.

(U//~~FOUO~~) After reviewing an email from POWELL with the subject line "Re: Question," CLINTON stated she did not want to guess precisely what POWELL was trying to say in paragraph three, but understood it to mean any communications of official business would be government records. This email did not factor into her decision to use a personal email account.

(U//~~FOUO~~) After reviewing an email dated February 1, 2009 with the subject line "Re: Follow up," CLINTON stated she did not continue to receive email at her AT&T address after transitioning to her clintonemail.com address. Some aides had access to CLINTON's BlackBerry and email accounts, but she did not recall specifically who had access. Additionally, CLINTON did not recall any specific routine for deleting email from her account while Secretary of State, nor did she recall ever receiving any messages

~~TOP SECRET~~~~SECRET~~b1  
b3

~~TOP SECRET~~~~FOUO~~b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 5  
indicating her account was reaching a storage limit. CLINTON was not aware of the specific details regarding the hardware, software, or security of the server hosting clintonemail.com. She occasionally received odd looking email, but never noticed an increase in these types of emails that would be a cause for concern. HUMA ABEDIN also had an account on clintonemail.com because she frequently assisted CLINTON with personal matters. CLINTON did not recall any other individuals being offered an account on clintonemail.com.

(U//~~FOUO~~) CLINTON stated at least a hundred, if not several hundred, State employees had her clintonemail.com address. Some communicated directly with her, while others went through her top level staff. When her top staff received information, the recipient would determine if the information should be forwarded to her. None of CLINTON's staff ever expressed a concern regarding the sensitivity of the content of these emails. CLINTON's practice was to email State staff at their state.gov accounts, but would sometimes send email to a staff member's personal account if state.gov was down.

(U//~~FOUO~~) After reviewing an email dated June 4, 2011 with the subject line "RE: Google email hacking and woeful state of civilian technology," CLINTON stated she did not recall the compromise of State employees' Gmail accounts. However, CLINTON did recall the frustration over State's information technology systems.

(U//~~FOUO~~) After reviewing a State communication dated June 28, 2011 with the subject line "Securing Personal E-mail Accounts," CLINTON stated all cables of a certain policy nature went out under her name and she did not recall this specific cable. Additionally, CLINTON did not recall this cable correlating with BRYAN PAGLIANO upgrading the clintonemail.com server. CLINTON did not consider switching to a state.gov account at this time, but did recall reports of compromises to state.gov systems. CLINTON understood the email system used by her husband's personal staff had an excellent track record with respect to security and had never been breached.

(U//~~FOUO~~) CLINTON was not involved in the decision to move from the Apple server managed by JUSTIN COOPER to a server built by BRYAN PAGLIANO. Therefore, CLINTON had no knowledge of the reasons for selecting to install it in the basement of CLINTON's New York residence or the hardware, software, and security protocols used to construct and operate the server. Furthermore, CLINTON did not have any conversations with regard to using the server to avoid the Freedom of Information Act (FOIA), and specifically denied using the server to avoid Federal Records Act (FRA) requirements. Based on her practice of emailing staff on their state.gov accounts, CLINTON assumed her communications were captured by State systems. CLINTON was not aware of State employee [redacted] [redacted] expressing concerns CLINTON's email server was not compliant with the FRA.

b6  
b7C

(U//~~FOUO~~) When CLINTON had technical issues with her email account, she contacted COOPER to resolve the issues. She could not recall ever contacting PAGLIANO for technical support. CLINTON recalled having issues with email during Hurricane Irene because cell phone systems were

~~TOP SECRET~~~~FOUO~~b1  
b3



~~TOP SECRET~~

~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 6

down; however, she could still receive email on her iPad. She did not recall using an iPad mini until after her tenure as Secretary of State and has never used a Macbook or other computer to access her email.

(U//~~FOUO~~) SIDNEY BLUMENTHAL is a longtime friend of CLINTON who frequently sent information he thought would be useful. CLINTON sometimes read and forwarded the information to appropriate personnel, but in other instances did not have the time to read his email. After reviewing an email dated January 31, 2011 with the subject line "hrc memo intel egypt 013111.docx," CLINTON stated [REDACTED] was a retired CIA officer, but she had no concerns regarding the sources of the memos being classified. CLINTON viewed the content as journalistic because BLUMENTHAL did not have a clearance and was not in government at that time. CLINTON did not request the memos, but commented BLUMENTHAL is a prodigious writer whose information was sometimes accurate and sometimes not. After reviewing an email dated June 24, 2012 with the subject line "Re: H: Here it is: latest, latest, intel on MB/SCAF inside deal. Sid," CLINTON commented it was a confusing time in Egypt and State was trying to obtain all of the intelligence it could on Egypt. However, she had no concerns regarding the classification of the email.

b3  
b7E

(S//~~AF~~) After reviewing an email dated October 13, 2012 with subject line "This am Green on Blue," CLINTON stated she did not remember the email specifically. CLINTON advised [REDACTED] was working at the DOD at the time of this communication, but had previously worked for the [REDACTED] was someone who was well acquainted with handling classified information and CLINTON described him as someone she held in high regard. Moreover, CLINTON relied on [REDACTED] and had no concern over his judgment and ability to handle classified information. CLINTON believed she would be speculating if she were to state what [REDACTED] meant when he referred to [REDACTED]

b3  
b7E

b1  
b3

[REDACTED] After reviewing an email dated [REDACTED] with subject line [REDACTED] CLINTON stated she did not remember the email specifically. CLINTON stated deliberation over a future drone strike did not give her cause for concern regarding classification. CLINTON understood this type of conversation as part of the routine deliberation process. Moreover, she recalled many conversations about future strikes that never occurred.

b1  
b3

[REDACTED] After reviewing an email dated [REDACTED] with subject line [REDACTED] CLINTON stated she did not remember the email specifically. [REDACTED]

b1  
b3

[REDACTED] CLINTON thought any attempt she made to determine [REDACTED] meaning would be speculation. After mentioning the names of the individuals on the displayed email, CLINTON stated they were experienced foreign service professionals and she had no reason to doubt their judgment and ability to handle classified information.

(S)

b1  
b3

~~TOP SECRET~~

~~TOP SECRET~~

b1  
b3



~~TOP SECRET~~~~FOUO~~b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 7

b1  
b3

[REDACTED]

[REDACTED] CLINTON viewed the email as a typical deliberation document and had no concerns the displayed email contained classified information. As it relates to classification, CLINTON stated the displayed email was forwarded to her and she relied on the judgment of the career foreign service officers and others in the "thick" of what was happening. CLINTON had no reason not to rely on the people she worked with at State. CLINTON did not recall JACOB SULLIVAN using his Google email account for official business and could not say why it was used in this instance.

[REDACTED] After reviewing an email dated [REDACTED] with subject line [REDACTED] CLINTON stated she did not remember the email specifically [REDACTED] CLINTON identified the portion of the email where [REDACTED] writes "let me know what you can via this channel" as being representative of the emphasis he placed on handling information appropriately. CLINTON had no concerns the displayed email contained classified information. CLINTON viewed this email as the State deliberation process to determine how to respond to a news report. During her tenure, CLINTON stated State did the best they could to not confirm drone strikes and were as careful as possible, but had to deal with a "rash" of news reports on drones. CLINTON did not recall a State policy on confirming classified information in media reports.

b1  
b3

(S/[REDACTED]) After reviewing an email dated August 25, 2010, with subject line "Fw: NY Times article on Salehi," CLINTON stated she did not remember the email specifically. CLINTON stated she was not concerned the displayed email contained classified information [REDACTED] but stated she had no reason to doubt the judgment of the people working for her on the "front lines."

b1  
b3

[REDACTED] After reviewing an email dated [REDACTED] with subject line [REDACTED] CLINTON stated she did not remember the email specifically. CLINTON thought [REDACTED] was a competent professional who served in some of State's most difficult posts. CLINTON relayed State did the best they could while considering the "constant barrage of press" trying to confirm drone strikes. CLINTON stated [REDACTED] must have believed this email was "SBU" because that was how he marked it. CLINTON understood SBU to mean Sensitive But Unclassified. CLINTON stated foreign-based US Embassies would have a SCIF with secure computers and phones to communicate sensitive information. [REDACTED]

b1  
b3

(S/[REDACTED]) After reviewing an email dated December 27, 2011, with subject line "FW: (SBU)," CLINTON stated she did not remember the email specifically. CLINTON was not concerned the displayed email contained classified information. CLINTON stated no policy or practice existed related to communicating around holidays and it was often necessary to communicate in code or do the best you could to convey the information considering the system you were using [REDACTED]

b1  
b3~~TOP SECRET~~~~FOUO~~b1  
b3

~~TOP SECRET~~~~(U//FOUO)~~b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton On 07/07/2016 Page 8

b1  
b3

[REDACTED] CLINTON did not see how this email would have "added more fuel to an already big fire." CLINTON believed the individuals sending the email thought the classification to be SBU and she trusted them to handle the information appropriately.

[REDACTED] After reviewing an email dated [REDACTED] with subject line [REDACTED] CLINTON stated she did not remember the email specifically. CLINTON was not concerned the displayed email contained classified information. CLINTON relied on the judgment of the people that worked for her to handle information appropriately. [REDACTED]

b1  
b3

(U//FOUO) After reviewing an email dated June 17, 2011, with subject line [REDACTED] [REDACTED] CLINTON stated she did not remember the email specifically. CLINTON stated a "nonpaper" was a document with no official heading, or identifying marks of any kind, that can not be attributed to the US Government. CLINTON thought a "nonpaper" was a way to convey the unofficial stance of the US Government to a foreign government and believed this practice went back "200 years." When viewing the displayed email, CLINTON believed she was asking SULLIVAN to remove the State letterhead and provide unclassified talking points. CLINTON stated she had no intention to remove classification markings. CLINTON had no recollection of actually receiving a "nonpaper" or a secure fax in this instance. [REDACTED] talking points are typically classified, but CLINTON did not recall in this instance.

b5 per DOS

(U//~~FOUO~~) After reviewing an email dated April 9, 2012, with subject line "Call to President Banda," CLINTON stated she did not remember the email specifically. When asked what the parenthetical "C" meant before a paragraph within the captioned email, CLINTON stated she did not know and could only speculate it was referencing paragraphs marked in alphabetical order. CLINTON could not say for sure if the parenthetical "C" is used for portion marking classified documents. CLINTON understood the top of the email is marked "Confidential" and asked the interviewing Agents if that was what "C" referenced. [Agent note: Email was marked as classified at the Confidential level by the FBI based on a determination by the OCA] When asked of her knowledge regarding Top Secret, Secret, and Confidential classification levels of US government information, CLINTON responded that she did not pay attention to the "level" of classified information and took all classified information seriously. CLINTON was not concerned the displayed email contained classified information. CLINTON believed the email amounted to a "condolence call" and questioned the classification level.

~~TOP SECRET~~~~(U//FOUO)~~b1  
b3

~~TOP SECRET~~~~FOUO~~b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton On 07/02/2016, Page 9

[REDACTED] CLINTON believed information should be classified in the case of covert military action, the use of sensitive sources and where sensitive deliberations took place. When asked whether CLINTON believed information should be classified if its unauthorized release would cause damage to national security, she responded, "yes, that is the understanding." CLINTON believed the classification level of future drone strikes depended on the context. CLINTON believed drone strikes to be an "important tool" but also a program frequently in the press [REDACTED]

b1  
b3

CLINTON believed the people at State did the best they could to deliberate about future strikes and respond to foreign governments and media after a strike occurred.

(U//~~FOUO~~) CLINTON stated she received no instructions or direction regarding the preservation or production of records from State during the transition out of her role as Secretary of State in early 2013. However, in December of 2012, CLINTON suffered a concussion and then around the New Year had a blood clot. Based on her doctor's advice, she could only work at State for a few hours a day and could not recall every briefing she received. CLINTON did not have any discussions with aides about turning over her email records, nor did anyone from State request them. She believed her work-related emails were captured by her practice of sending email to the state.gov email addresses of her staff. CLINTON was unaware of the requirement to turn over printed records at that time. Her physical records were boxed up and handled by aides.

(U//~~FOUO~~) After reviewing an email dated December 11, 2012 with the subject line "FW: Significant FOIA Report," CLINTON stated she did not recall the specific request and was not aware of receiving any FOIA requests for information related to her email during her tenure as Secretary of State. State had a FOIA department and CLINTON relied on the professionals in that department to address FOIA matters.

(U//~~FOUO~~) Shortly after leaving State, representatives from State came to her residence and removed communications and other equipment they had installed to facilitate her duties as Secretary of State. CLINTON did not recall being read-out of her clearance or any SAPs by State personnel.

(U//~~FOUO~~) CLINTON's email address was publicly disclosed in March 2013 when BLUMENTHAL's email account was compromised. As a result, CLINTON was advised to change her email address and did so, but she did not recall specifically who made this recommendation.

(U//~~FOUO~~) Regarding the transition from the Pagliano server to a server operated by Platte River Networks (PRN), CLINTON recalled her husband's staff wanted a higher level of service than could be provided by the Pagliano server. This transition was likely handled by one of her husband's aides. JUSTIN COOPER.

(U//~~FOUO~~) In the Fall of 2014, CLINTON recalled receiving a letter from State which was also sent to former Secretaries of State COLIN POWELL, CONDOLEEZZA RICE, and MADELEINE

~~TOP SECRET~~~~FOUO~~b1  
b3

~~TOP SECRET~~~~NOFORN~~b1  
b3Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 10

ALBRIGHT. From the letter, CLINTON understood State was concerned there were gaps in their records and requested CLINTON's assistance in filling those gaps. CLINTON wanted to assist State, so she directed her legal team to assist in any way they could. CLINTON expected her team to provide any work-related or arguably work-related emails to State; however, she did not participate in the development of the specific process to be used or discussions of the locations where her emails might exist. Additionally, CLINTON was not consulted on specific emails as to their content being work-related or not. CLINTON did not have any conversations regarding procedures if any potentially classified information was discovered during the review of her emails because she had no reason to believe classified information would be found in her email account.

(U//~~FOUO~~) After reviewing an email dated November 26, 2010 with the subject line "MbZ call -- 7:15am," CLINTON stated she recalled the time period of the WikiLeaks disclosures because it was a difficult time for State. She spent long hours on the phone with foreign diplomats addressing the WikiLeaks disclosures and ensuring no one was in danger as a result of the disclosures. Regarding the specific email, CLINTON did not know why it was not in the approximately 30,000 emails produced to State and, based on its content, would expect it to be considered work-related.

(U//~~FOUO~~) In December 2014, after her staff completed their response to the request from State for her email records, CLINTON was asked what she wanted to do with her personal emails. She told her staff she did not need them anymore. In or around this same timeframe the retention policy for her email was changed as part of her move to a new personal office account.

(U//~~FOUO~~) CLINTON transitioned to an email address on the hrcoffice.com domain because she had a small number of personal staff, but no physical office or common email domain. To address these issues, she moved to a common email domain and physical office space. After this move, CLINTON did not recall any further access to clintonemail.com.

(U//~~FOUO~~) CLINTON never deleted, nor did she instruct anyone to delete, her email to avoid complying with the Federal Records Act, FOIA, or State or FBI requests for information. Concerning the Congressional preservation request on March 3, 2015 for email and other records, CLINTON trusted her legal team would comply with the request.

(U//~~FOUO~~) CLINTON had no knowledge regarding the following topics:

- The creation, storage, transfer, or access to an archive of her email created by MONICA HANLEY in the Spring of 2013
- The specific processes and procedures used by CLINTON's legal team and PRN to separate her work and personal email
- Discussions of federal records related to the Apple, Pagliano, or PRN servers

~~TOP SECRET~~~~NOFORN~~b1  
b3

~~TOP SECRET~~

~~OC/NF~~

b1  
b3

Continuation of FD-302 of Interview of Hillary Rodham Clinton, On 07/02/2016, Page 11

- The existence of any copies of her clintonemail.com emails, other than what has been provided to the FBI and State
- March 2015 deletions by PRN

~~TOP SECRET~~

~~OC/NF~~

b1  
b3

~~TOP SECRET~~ [REDACTED] ~~NT~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 02/29/2016

(U//FOUO) On February 26, 2016, [REDACTED] DOB [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at the FBI Washington Field Office, 601 4<sup>th</sup> Street NW, Washington DC. Present for the interview was [REDACTED] counsel, [REDACTED] Attorney at Law, at [REDACTED] [REDACTED], as well as [REDACTED] and [REDACTED], from the Department of Justice (DOJ) Counterintelligence and Export Control Section. Prior to the interview [REDACTED] agreed to sign a non-disclosure agreement in anticipation of viewing classified documents during the interview. After being advised of the identities of the interviewing agents, and the purpose of the interview, [REDACTED] provided the following information:

b6  
b7C

(U//FOUO) [REDACTED] became the U.S. Department of State (DoS) [REDACTED] [REDACTED] under [REDACTED] He continued to serve as the [REDACTED] under [REDACTED] [REDACTED] became the [REDACTED] under [REDACTED] before being named the [REDACTED]. As the [REDACTED] office was located in Washington DC but he traveled frequently and took trips to Afghanistan and Pakistan every four to six weeks.

b6  
b7C

(U//FOUO) [REDACTED] did not have frequent contact with the Secretary of State when [REDACTED]. This was because [REDACTED] handled all of the direct communications with the Secretary and her team himself. [REDACTED] described his role under [REDACTED] as being external facing. He further explained that he was responsible for coordinating with Congress and facilitating other international and economic engagements. [REDACTED] became more focused on Afghanistan matters when [REDACTED] became the [REDACTED] because [REDACTED] wanted to focus mainly on Pakistan. In this role, [REDACTED] had more regular contact with the Secretary and her team, which included traveling to the region with them.

b6  
b7C

(U//FOUO) [REDACTED] provided that he primarily interacted with the following individuals on the Secretary's team: CHERYL MILLS for USAID and communications matters; JAKE SULLIVAN for policy matters and to prepare for Deputy Committee or Principal Committee meetings; HUMA ABEDIN for logistics; and [REDACTED] for communications matters. [REDACTED] noted that he has [REDACTED]

b6  
b7C

Investigation on 02/26/2016 at Washington DC

File # [REDACTED] Date dictated N/A

By SA [REDACTED] SA [REDACTED]

b3  
b7E

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~ [REDACTED] ~~NT~~

b1  
b3

b1  
b3

~~TOP SECRET~~ [REDACTED] ~~AT~~

Continuation of FD-302 of [REDACTED] Interview of [REDACTED] On 02/26/2016 Page 2

b6  
b7C

(U//FOUO) [REDACTED] communicated directly with SULLIVAN and MILLS for anything that needed the Secretary's attention. Examples include topics that involved international matters, topics that could potentially impact DoS equities, and topics involving private sector engagements. These exchanges could be either classified or unclassified depending on the specific content and were done via the appropriate telephone or email system.

b6  
b7C

(U//FOUO) While at DoS, [REDACTED] had an OpenNet and ClassNet account but he did not have a JWICS account. DoS also issued [REDACTED] a Blackberry, which was linked to his unclassified DoS email account, and a STE for his home. [REDACTED] used his Blackberry email extensively when he was overseas because other communication channels were often not available.

b6  
b7C

(U//FOUO) [REDACTED] could only recall one instance following the birth of his son when he received an email directly from the Secretary. He remembered that the email came from a non-DoS email account but he didn't think much of it at the time. [REDACTED] was not aware that the Secretary was using a private email account and server to conduct DoS business, nor was [REDACTED] aware of any other DoS employees using personal email accounts for official business. [REDACTED] provided that he had the personal email addresses of both SULLIVAN and MILLS but he did not recall ever using those accounts for official business.

b6  
b7C

[REDACTED] confirmed that he was read into a Special Access Program [REDACTED] understood the sensitivities surrounding the program and the need to appropriately safeguard related information. As such, the DoS stance was not to publicly comment on the program.

b1  
b3

[REDACTED]

b1  
b3

[REDACTED] was shown a copy of an email chain from December of 2011 with the subject "(SBU)." After reviewing the email [REDACTED] stated that he did not remember the circumstances in which the email was originally sent. However, based on the email time stamp [REDACTED] believed he was in California when he received the email and that he would not have had any other means of forwarding the information to those who needed it. [REDACTED] stated that

b1  
b3

~~TOP SECRET~~ [REDACTED] ~~AT~~

b1  
b3

~~TOP SECRET~~~~NP~~

Continuation of FD-302 of [redacted] Interview of [redacted] On 02/26/2016, Page 3  
sending information on the unclassified system was not ideal but that he often

b6  
b7C

did not have a choice when it came to time sensitive information. [redacted] did not recall receiving any specific training or guidance on how time sensitive information should be transmitted.

b1  
b3

[redacted] was shown a copy of an email chain from February of 2012 with the subject "Alert." [redacted] did not remember the email chain. However, after reviewing the email he stated that [redacted]

b1  
b3

[redacted] Nonetheless, [redacted] did not have concerns sending this type of information on an unclassified system because the story was about to break in the news and it was important that they got the information to the Secretary before that occurred.

[redacted] was shown a copy of an email chain from [redacted] with the subject [redacted] stated it was sent prior to the referenced article being released in the press. [redacted] could not recall any further details about the information provided in the email. He noted that a number of similar stories were being released by the press at that time. [redacted] believed that the information in the email could be treated as unclassified because the article was about to be released and it was critical that he notify the appropriate people within DoS.

b1  
b3

[redacted] was shown a copy of an email chain from [redacted] with the subject [redacted] provided that the email was forwarding a news article of interest to individuals within DoS. [redacted] stated that the comments he included when he forwarded the email were not meant to confirm the veracity of the news article but rather to express his frustration with the article. [redacted] further explained that 2011 was a particularly difficult period for bilateral relationships in the region and that DoS efforts were often complicated by such articles.

b1  
b3

[redacted] was shown a copy of an email chain from May of 2011 with the subject "Update." [redacted] did not recall the exact circumstances of the email but noted that it was unusual for him to interact directly with [redacted] provided that he forwarded the email because it was a matter that required the immediate attention of DoS to preserve its equities.

b1  
b3

(U//FOUO) At the conclusion of the interview [redacted] noted that none of the emails that he was shown were originated by him. The emails either involved information that was about to be released publicly or were authored by another individual.



b6  
b7C~~TOP SECRET~~~~NP~~b1  
b3



~~TOP SECRET~~



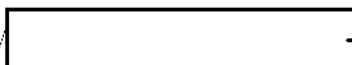
b1  
b3

Continuation of FD-302 of ..... Interview of  ..... On 02/26/2016, Page 4  
(U//~~FOUO~~) A copy of the original interview notes and the NDA signed by  are enclosed in a  
1A envelope.

b6  
b7C

b6  
b7C

~~TOP SECRET~~



b1  
b3

~~CONFIDENTIAL~~

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/4/2016

(U//~~FOUO~~) On February 3, 2016, [ ] telephone number [ ] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [ ] and [ ] at the offices of [ ] Washington, DC. Also present for the interview was [ ] an [ ] Principal, whom [ ] asked to sit in on the interview. After being advised of the identities of the interviewing agents, and the purpose of the interview, [ ] provided the following information:

b6  
b7C

(U//~~FOUO~~) [ ]

b6  
b7C

(U//~~FOUO~~) [ ] office at DoS was located on "Mahogany Row," a term given to the Executive hallway where the Secretary of State's office is also located. [ ] held a Top Secret (TS), Sensitive Compartmented Information (SCI) clearance while at DoS, and handled classified information on a daily basis. [ ] received copies of the Presidential Daily Brief (PDB), the dissemination of which was restricted to only the highest positions in the United States Government.

b6  
b7C

(U//~~FOUO~~) When [ ] needed to communicate something classified to CLINTON, [ ] would walk down "Mahogany Row" and talk to CLINTON face-to-face. If CLINTON was not in the office, or on travel, and [ ] needed to discuss classified information, [ ] would contact CLINTON via a secure phone or send her a secure memo.

b6  
b7C

(U//~~FOUO~~) [ ] was not aware that CLINTON was using a personal email account while she was Secretary of State, nor did [ ] recall what address [ ] typed in or saw when [ ] sent emails to or received emails from CLINTON. [ ] assumed whatever devices CLINTON used to conduct business while she was Secretary of State were approved, because nobody at DoS used devices without approval. [ ] was not aware of any DoS policy against using personal or private email accounts to conduct unclassified DoS business.

b6  
b7C

Investigation on 2/3/2016 at Washington, D.C.

File # [ ]-302 Date dictated N/A

b3  
b7E

By SA [ ] SA [ ]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 2/3/2016, Page 2

b6  
b7C

(U//~~FOUO~~) On a few occasions, \_\_\_\_\_ traveled with CLINTON. However, the majority of \_\_\_\_\_ travel while \_\_\_\_\_ was \_\_\_\_\_ was done so on \_\_\_\_\_ own.

b6  
b7C

(U//~~FOUO~~) Agents asked \_\_\_\_\_ a 2013 speech to the American Foreign Service Association, \_\_\_\_\_

b6  
b7C

\_\_\_\_\_

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ explained the quote was in response to a question \_\_\_\_\_ in regards to how business had changed at DoS since \_\_\_\_\_ PRESIDENT CLINTON's administration. \_\_\_\_\_ further explained that during \_\_\_\_\_ previous assignment to DoS \_\_\_\_\_ nobody at DoS had access to unclassified systems of any sort. Blackberries didn't exist, and unclassified computer systems were not yet installed at DoS. The only way to communicate during that time period was via cables and on the telephone. In contrast, when \_\_\_\_\_ returned to DoS in \_\_\_\_\_ had access to SIPRNet, JWICS, and Unclassified computers, as well as unclassified Blackberries, and secure iPads. \_\_\_\_\_ the above statement, \_\_\_\_\_ was trying to explain how technology has allowed for a different form of information flow, and ultimately sped up the way in which DoS does business.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ further clarified \_\_\_\_\_ referenced above in \_\_\_\_\_ 2013 speech, was unclassified, \_\_\_\_\_ was not implying that information CLINTON may have been communicating classified material on her Blackberry concerning the unclassified matter.

b6  
b7C

(U//~~FOUO~~) It was \_\_\_\_\_ opinion that everybody at DoS takes security very seriously and understands the importance of protecting sources and methods. \_\_\_\_\_ hinks there is a misconception about how DoS classifies documents, and further explained that generally the only way to discuss topics with Foreign Partners is via unclassified channels, or in very sensitive cases, by making arrangements to meet in person at Embassies or at DoS. Since there isn't a classified system that allows DoS to communicate with its foreign counterparts, conversations that are held with foreign partners in unclassified channels are later "up-classified" to Secret to protect the information.

b6  
b7C

(U//~~FOUO~~) In defense of DoS practices, \_\_\_\_\_ shared a story concerning \_\_\_\_\_ interaction with then FBI Deputy Director MARK GIULIANO, wherein \_\_\_\_\_ stated \_\_\_\_\_ interacted frequently with GIULIANO via email. \_\_\_\_\_ stated \_\_\_\_\_ had the upmost respect for GIULIANO, but believed if \_\_\_\_\_ was to review \_\_\_\_\_ unclassified email exchanges with GIULIANO, \_\_\_\_\_ would find emails that some would consider sensitive.

b6  
b7C

~~CONFIDENTIAL~~

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 2/3/2016, Page 3

b6  
b7C

(U//~~FOUO~~) When \_\_\_\_\_ received a request to produce documents in response to Freedom of Information Act (FOIA) inquiries, \_\_\_\_\_ also queried and produced emails from \_\_\_\_\_ personal Gmail account that \_\_\_\_\_ determined were "even remotely related to work." \_\_\_\_\_ sometimes sent short emails to \_\_\_\_\_ family via Gmail while \_\_\_\_\_ was on travel and felt that if \_\_\_\_\_ referenced negotiations or anything concerning \_\_\_\_\_ role at DoS, \_\_\_\_\_ should produce the documents in an abundance of caution. \_\_\_\_\_ further explained that it was not uncommon for \_\_\_\_\_ to have to use \_\_\_\_\_ personal Gmail account to communicate while on travel, because there were often times \_\_\_\_\_ could not access her DoS unclassified account. \_\_\_\_\_ would try to copy her DoS email account on any DoS related communications \_\_\_\_\_ may have sent from her Gmail account.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was not aware of any specific instances where \_\_\_\_\_ received notification concerning a potential hack of any of \_\_\_\_\_ email accounts (DoS or personal) or the email accounts of other DoS employees. However, \_\_\_\_\_ explained \_\_\_\_\_ was sure people tried to hack into \_\_\_\_\_ personal email account and the accounts of \_\_\_\_\_ team approximately two years ago during \_\_\_\_\_ in the Iran negotiations. Specifically, \_\_\_\_\_  
\_\_\_\_\_ received a similar email. \_\_\_\_\_ reported the incident to DoS Diplomatic Security who reportedly traced the emails back to a \_\_\_\_\_

b6  
b7C

b1 per DOS

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/17/2015

(U//~~FOUO~~) [redacted] date of birth [redacted] was interviewed at the offices of PLATTE RIVER NETWORKS (PRN), 5700 Washington Street, Denver, Colorado 80216, by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and [redacted]. Also present during the interview were [redacted] attorney, U.S. Department of Justice and [redacted] attorney at [redacted]. After being advised of the identity of the interviewing agents, and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) In mid-2013, [redacted] was selected to provide technical support on a contract PRN had acquired for the management of a new server used solely for email exchange for domains and accounts associated with BILL CLINTON, HILLARY CLINTON and their aides under the PRN account name CESC (CESC client). [redacted] knew the company InfoGrate to be the contact who initiated the PRN contract with the CESC client. [redacted] understood the CESC client was already using email domains hosted on a server out of their residence in Chappaqua, New York, and in order to effect the transition to the PRN managed new server, [redacted] needed to understand the needs of the client and the configuration of the server being housed in Chappaqua. [redacted] was put in contact with BRYAN PAGLIANO, who [redacted] understood to be the administrator of the server in Chappaqua. PAGLIANO granted [redacted] remote administrator access to the server under the administrator user name [redacted] and in mid-2013, [redacted] logged in to the server at Chappaqua.

b6  
b7C

(U//~~FOUO~~) [redacted] described the physical equipment comprising the email server at the Chappaqua residence as a Dell PowerEdge 2900 (PowerEdge 2900) running Microsoft Exchange 2007, a Dell PowerEdge 1950 (PowerEdge 1950) being solely used as a BlackBerry Enterprise Server (BES), a Cisco NSS 324 for Network Attached Storage (NAS), a switch, a firewall and a Uninterruptible Power Supply (UPS). The PowerEdge 2900 server hosted the email domain presidentclinton.com, wjcoffice.com and clintonemail.com, and had 20 to 30 email accounts associated. The PowerEdge 2900 was used exclusively for email, with no file or print options. The PowerEdge 2900 had Microsoft Forefront security and Norton Symantec anti-virus software installed on it. No one but PAGLIANO had administrator rights to the PowerEdge 2900 server. [redacted] believed the Chappaqua residence had Comcast as an Internet Service Provider (ISP).

b6  
b7C

(U//~~FOUO~~) In order to effect the transition from the foregoing server equipment in the CLINTON's residence in Chappaqua to the new PRN server infrastructure and service, CESC and PRN

---

Investigation on 09/15/2015 at Denver, ColoradoFile # [redacted] 302 Date dictated N/Ab3  
b7EBy SA [redacted] SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 09/15/2015, Page 2b6  
b7C

arranged a time to power down the equipment in Chappaqua, transport it to a data center and migrate the existing email accounts and domains to the new server infrastructure being provided by PRN.

(U//~~FOUO~~) On or around 06/22/2013, and based on an infrastructure plan as part of a Service Level Agreement (SLA) to provide the CLINTONs with new hardware, [REDACTED] a PRN employee, setup a Dell PowerEdge 620 (PowerEdge 620), two PowerConnect 2824 switches, two Fortinet firewalls and a Datto SIRIS 2000 (DATTO), and hooked them up in a rented space at Equinix, a data center located in Secaucus, New Jersey.

b6  
b7C

(U//~~FOUO~~) On 06/23/2013, [REDACTED] traveled to the CLINTON residence in Chappaqua and picked up the PowerEdge 2900, the PowerEdge 1950, and the NAS, while leaving the switch, firewall and UPS at the residence. [REDACTED] transported the equipment to the same rented space at Equinix as the PowerEdge 620, where [REDACTED] plugged in and networked all the equipment to get it back online in order to provide CESC with continued email access. [REDACTED] plugged in the NAS, but according to [REDACTED] no email archiving or back-up was on it and it appeared to only have install files. The NAS was not configured to archive email by [REDACTED] or PRN at any time. [REDACTED] changed the mail exchanger (MX) record to specify the transition to the new IP address and configuration at Equinix.

b6  
b7C

(U//~~FOUO~~) On or around 06/30/2013, [REDACTED] began the email migration for all CESC accounts from the PowerEdge 2900 to the PowerEdge 620. [REDACTED] performed this by right-clicking on individual mailboxes and migrating them over one at a time. [REDACTED] stated he brought over the entire content of all the mailboxes from the PowerEdge 2900 to the PowerEdge 620 as there was no way to do it "piece meal" or partially. [REDACTED] described the migration process as more of a "sync" and once the servers "agree" that the mailbox is moved, the mailbox is removed from the old server. As a result of the migration, no email content existed on the PowerEdge 2900. During the migration, the PowerEdge 2900 and 620 worked together in the same exchange, where the servers agree that each email sent or received is an identical copy. Additionally, [REDACTED] configured the PowerEdge 620 to host a Blackberry Enterprise Server (BES) and a Domain Controller as virtual machines. [REDACTED] explained the Domain Controller as being used for password and authentication requests. The PowerEdge 620 was also running Microsoft Exchange 2010 software, which was an upgrade from the software on the PowerEdge 2900. Additionally, as part of the new server infrastructure provided by PRN, [REDACTED] configured the DATTO back-up device to take multiple snapshots of the server a day that purged at 60 day intervals. [REDACTED] also configured both sets of firewalls and switches for redundancy in case one went down. After several days of migration, the PowerEdge 620 had all email mailboxes migrated to it and was processing email on Microsoft Exchange 2010 for the email domains presidentclinton.com, wjcoffice.com and clintonemail.com. [REDACTED] was "very confident" that all email had migrated from the PowerEdge 2900 to the PowerEdge 620. At some point later, [REDACTED] remembers adding the domain [REDACTED] to the PowerEdge 620. After total migration, PRN decided to keep the PowerEdge 2900, 1950 and NAS running, even though it was no

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 09/15/2015, Page 3b6  
b7c

longer processing email, in order to ensure email was being delivered without failure through the PowerEdge 620. There was no official user security policy to have an account on the PowerEdge 620. [REDACTED] registered the Secure Sockets Layer (SSL) certificate for the domains hosted on the PowerEdge 620. Additionally, PAGLIANO gave [REDACTED] the credentials for the clintonemail.com domain, registered at Network Solutions.

b6  
b7c

(U//~~FOUO~~) On or around 12/2013, PRN made the decision that email delivery was working well after the migration from the PowerEdge 2900 to the PRN managed PowerEdge 620. In order to power down the PowerEdge 2900, [REDACTED] stated Microsoft Exchange 2007 would need to be uninstalled from the PowerEdge 2900, or the PowerEdge 620 would generate error messages. [REDACTED] uninstalled Microsoft Exchange 2007 from the PowerEdge 2900 by clicking on uninstall and following the system prompted checks to ensure there were no ties between the PowerEdge 2900 and the PowerEdge 620 and no active mailboxes were on the PowerEdge 2900. From that point on, the PowerEdge 2900, 1950 and NAS sat disconnected in the cage at Equinix until the FBI picked up the PowerEdge 2900 on 08/12/2015. The uninstallation of Microsoft Exchange and powering down of the PowerEdge 2900 was an action taken by PRN as standard protocol without order or direction from the CESC client.

b6  
b7c

(U//~~FOUO~~) Based on his experience, [REDACTED] described PAGLIANO's set-up on the PowerEdge 2900 as a standard email set-up. [REDACTED] also described his set-up on the PowerEdge 620 as standard. Moreover, [REDACTED] described that email messages accepted by the PowerEdge 620 would first go through MX Logic, a third party company that removes viruses and spam before sending the message through Giglinx, the Internet Service Provider (ISP) at Equinix. From there, [REDACTED] could not recall if the email would go through CloudJacket or the firewall, but he knew they were in succession. CloudJacket was an appliance used for intrusion prevention on the PowerEdge 620. CloudJacket had pre-configured settings that would block or blacklist certain email traffic it identified as potentially harmful. Occasionally, CloudJacket would send email notifications to [REDACTED] as the system administrator, prompting him to block certain IP addresses. [REDACTED] described these notifications as normal and could not recall any serious security incident or intrusion attempt that he was aware of. [REDACTED] could not identify any IP addresses, or their country of origin, that were involved in a brute force attack (BFA) against the PowerEdge 620. Email traffic would then go through the switch and to the PowerEdge 620 where it would be processed by Microsoft Exchange 2010. Additionally, [REDACTED] installed Trend Micro AntiVirus and later, Webroot AntiVirus.

b6  
b7c

(U//~~FOUO~~) [REDACTED] stated the CESC client originally requested to encrypt email such that no one but the user could read the content. This, ultimately, was not the way the email was configured so that system administrators could troubleshoot all problems occurring within user accounts. [REDACTED] recalled [REDACTED] and [REDACTED] as having system administrator rights to the PowerEdge

b6  
b7c

Continuation of FD-302 of Interview of [REDACTED], On 09/15/2015, Page 4b6  
b7C

620, although [REDACTED] believed he handled almost all issues entirely, [REDACTED] was seldom used, if at all, for work on CESC. System administrators could move mailboxes, change and reset passwords, and sometimes view email for archive searches when the users didn't have the time and CESC requested PRN complete the task. After PRN took control of the server, the CESC client never requested another individual have administrator access. [REDACTED] stated BRYAN PAGLIANO's password for the PowerEdge 2900 was changed and he did not have access to the PowerEdge 620. The CESC client did request 24 hour access to someone who could assist with any issues that should arise regarding their email accounts. In order to meet this request, PRN contracted with Level Platforms or Managed Workplace, a third-party company used for troubleshooting and help desk related issues for any late night or off-hour requests that [REDACTED] could not handle. The third-party company did not have administrator access to the server or email content, but could provide assistance with troubleshooting devices, connectivity to the server and password resets. [REDACTED] stated the help desk service was not used often and the CESC client would contact him directly. [REDACTED] was unsure, but thought the third party help desk service was no longer contracted with PRN for CESC client help.

b6  
b7C

(U//~~FOUO~~) In or around 02/2014, [REDACTED] was contacted by someone from CESC, that he recalled as [REDACTED] Last Name Unknown (LNU), informing him that she was going to ship him a MacBook containing a folder with old HILLARY CLINTON emails. [REDACTED] recalled no other identifying information regarding the MacBook. [REDACTED] recalled the MacBook being shipped via FedEx to his personal residence in [REDACTED] but does not recall any other information regarding the shipment. Once [REDACTED] received the MacBook, he identified the folders containing the HILLARY CLINTON email and recalled five subfolders being labeled 2009 through 2014. [REDACTED] did not recall the specific HILLARY CLINTON email account the tranche was from. [REDACTED] created a local storage folder under the address [hrcarchive@clintonemail.com](mailto:hrcarchive@clintonemail.com) and copied the pst files to it. The [hrcarchive@clintonemail.com](mailto:hrcarchive@clintonemail.com) account was not configured to send or receive email messages. [REDACTED] or someone from CESC, requested that only HILLARY CLINTON and two associates be granted access, but [REDACTED] could not recall the names of the associates. [REDACTED] shipped the foregoing MacBook back to [REDACTED] LNU, but recalled nothing about the return shipment.

b6  
b7C

(U//~~FOUO~~) In or around 09/2014, [REDACTED] was contacted by CLINTON aide CHERYL MILLS requesting [REDACTED] perform an archive search of all HILLARY CLINTON email, during her tenure as Secretary of State, from 01/2009 to 02/2013, sent to or received from an email address ending in .gov. It was originally requested that [REDACTED] burn the foregoing archive search to a DVD and FedEx it to CHERYL MILLS. Instead of that transmittal, [REDACTED] conducted the foregoing archive search, zipped the resulting .pst email files, encrypted them with AES256, and used a Secure File Transfer Protocol (SFTP) to transfer the files to the workstations of CHERYL MILLS and HEATHER SAMUELSON. Additionally, [REDACTED] password protected the pst files. Sometime shortly after, CHERYL MILLS contacted [REDACTED] and asked him to perform another archive search for all email on all accounts in HILLARY CLINTON's mailbox during her tenure as Secretary of State.

b6  
b7C



Continuation of FD-302 of Interview of [REDACTED], On 09/15/2015, Page 5b6  
b7C

[REDACTED] conducted the requested archive search and transmitted it to MILLS and SAMUELSON using the same process, an SFTP transfer using AES256 encryption to their personal workstations.

[REDACTED] knew no additional detail regarding the workstations of MILLS and SAMUELSON.

b6  
b7C

Additionally, the archive search conducted by [REDACTED] did not contain email from the local storage folder hrcarchive@clintonemail.com.

(U//~~FOUO~~) In or around 12/2014, [REDACTED] was put in touch with an individual named [REDACTED] by someone from the CESC client. [REDACTED] informed [REDACTED] that HILLARY CLINTON and HUMA ABEDIN were going to have new email accounts on a new domain hosted on another server not administered by PRN. [REDACTED] informed [REDACTED] that HILLARY CLINTON's new email address was [REDACTED]@hrcoffice.com and HUMA ABEDIN's new email address was [REDACTED]@hrcoffice.com. [REDACTED] requested that [REDACTED] begin forwarding the email from HILLARY CLINTON's hrod17@clintonemail.com account, hosted on the PowerEdge 620, to her new [REDACTED]@hrcoffice.com account, hosted on another server unknown to [REDACTED] nor anyone from the CESC client, requested [REDACTED] to transfer any archived email to the new server referenced by [REDACTED] was not aware of any detail related to the new server referenced by [REDACTED] to include who managed it or what it was being used for.

b6  
b7C

(U//~~FOUO~~) In or around 03/2015, [REDACTED] was contacted by CESC with a request to inventory the CESC mailboxes to determine what exists, where it was stored and how it was backed up. [REDACTED] talked with [REDACTED] to coordinate the request and it was decided [REDACTED] would travel to Equinix to ensure the PowerEdge 2900, 1950 and NAS contained no email data. Once onsite at Equinix, [REDACTED] powered on the PowerEdge 2900, 1950 and NAS and verified no old email data or backups existed. When [REDACTED] returned to Equinix in 08/2015 to provide the PowerEdge 2900 to the FBI, he powered it up to check for any email or backup data. The 08/2015 inventory by [REDACTED] was not requested by anyone from CESC and was a step taken by PRN.

b6  
b7C

(U//~~FOUO~~) [REDACTED] stated all email accounts on the PowerEdge 620 had some back-up policy. Everything on the PowerEdge 620 was backed up through the DATTO device by taking several snapshots of the server daily and maintaining the data for 60 days. Additionally, all accounts had some back-up set by the user in their individual email client settings. Users could also archive email locally, by making .pst files on their computer workstation for example [REDACTED] stated the server just presents the email to the user – after that, the user could do whatever they want with the email. [REDACTED] did not know what any CESC client individual email user's setting was. Additionally, in or around 08/06/2015, PRN was made aware that DATTO was syncing with the DATTO cloud and storing email data related to CESC off-site. This off-site logging to DATTO's datacenter was not requested by PRN or CESC. Once the DATTO offsite logging was discovered, DATTO disabled the offsite logging feature leaving DATTO with 60 days of CESC email back-up from the day it was disabled. [REDACTED] believed DATTO was preserving the offsite email data.

b6  
b7C

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 09/15/2015, Page 6

(U//~~FOUO~~) \_\_\_\_\_ was shown a list of CESC email accounts provided to the FBI by PRN. \_\_\_\_\_ recognized most of the email accounts and knew that some were added and deleted throughout the life of the contract, but couldn't give a timeframe for the addition/deletions and wasn't aware of all of the users for each account. Additionally, \_\_\_\_\_ was unaware of the devices used by each user. When CESC users would acquire a new mobile device, they could configure it themselves due to Microsoft ActiveSync technology on the mobile device. On rare occasions, \_\_\_\_\_ would have to assist old blackberry users with synchronization with the BES.

b6  
b7C

(U//~~FOUO~~) PRN set-up a share folder on the PRN network for all documentation related to the CESC client. \_\_\_\_\_ believed PRN took this step to limit the individuals at PRN that had access to information regarding the CESC client.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ believed that PRN never used the company Techno+Rescue to recycle any equipment related to the CESC account. \_\_\_\_\_ believed that PRN never used Veeam software or service to backup the PowerEdge 620.

b6  
b7C

(U//~~FOUO~~) PRN never took action to purge or delete CESC email data from the PowerEdge 620 or DATTO. CESC never requested that PRN purge or delete email data associated with their account.

(U//~~FOUO~~) \_\_\_\_\_ was aware of no discussions with CESC regarding classified information or retention of federal records.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/04/2016

(U//~~FOUO~~) On February 18, 2016, [redacted] date of birth [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] at the offices of Platte River Networks (PRN), 5700 Washington Street, Denver, CO. Also present for the interview were SA [redacted] Information Technology Specialist/Forensic Examiner [redacted] Department of Justice (DOJ) Attorney [redacted] and [redacted] from [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

(U//~~FOUO~~) MONICA HANLEY contacted [redacted] via email on or about February 2014 regarding email belonging to HILLARY CLINTON. The email was stored on a Macbook and CLINTON did not want to lose the email, so HANLEY requested [redacted] transfer it to the Clinton Executive Services Corporation (CESC) server (Server) managed by PRN. The Server housed four virtual machines: a Microsoft Exchange server, a BlackBerry enterprise server, an administrative server, and a domain controller. [redacted] attempted to accomplish the task via a remote session using a remote support application called ScreenConnect. However, [redacted] was unable to import the files using ScreenConnect since the email was stored in the Macbook's Mail program. Therefore, [redacted] had HANLEY ship him the Macbook so he could import the mail files manually.

b6  
b7C

(U//~~FOUO~~) Upon receipt of the Macbook, [redacted] reviewed the files and noticed there were several mail folders and each was labeled with a different year from 2009-2013. He then conducted a Google search to identify an appropriate method for converting the Mac Mail files into .pst files. [redacted] believed he used Gmail as a way to convert the Mac Mail files to a format that could be imported into the Microsoft Exchange server. Once the conversion was complete, he created a new mailbox named HRC Archive. It was likely a regular Microsoft Exchange mailbox that could send and receive email. [redacted] did not recall who had access to the mailbox. Once the import onto the Server was successful, he deleted the email from the Macbook, but did not use any data wiping tools on the Macbook. [redacted] never deleted the HRC Archive mailbox from the Server and believed it should still exist there today; however, users with access to the mailbox could have altered its contents.

b6  
b7C

Investigation on 02/18/2016 at Denver, Colorado

File # [redacted] 302 Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 2

(U//~~FOUO~~) In April 2014, \_\_\_\_\_ remotely instructed \_\_\_\_\_ how to access the HRC Archive mailbox using Microsoft Outlook on her computer. \_\_\_\_\_ likely provided this assistance using the ScreenConnect application.

(U//~~FOUO~~) After reviewing several documents dated in and around July 23, 2014, \_\_\_\_\_ stated in July 2014 he had a conversation with CHERYL MILLS during which she requested \_\_\_\_\_ export a .pst file with all email in CLINTON's mailbox that was sent to or received from a .gov email address (July Export). After reviewing a list of .pst files modified in or around the same time, \_\_\_\_\_ opined he might have attempted the July Export using different tools, such as Outlook or PowerShell. He did not recognize the file name export.pst. After completing the July Export and verifying it would open correctly in Outlook, \_\_\_\_\_ burned DVDs of the files and arranged for a FedEx pickup the next day. However, MILLS subsequently requested a secure electronic transfer of the files instead of shipping physical media. Once the secure electronic transfer was complete, \_\_\_\_\_ destroyed the DVDs by breaking them in half.

(U//~~FOUO~~) After reviewing a July 24, 2014 email from BRYAN PAGLIANO regarding a regular expression text editor, \_\_\_\_\_ explained when a user changes his or her email address, Outlook updates the old email address with the new email address. MILLS was concerned CLINTON's then-current email address would be disclosed publicly and would be different from the one CLINTON was using at the time the emails were actually sent. \_\_\_\_\_ and PAGLIANO discussed using a regular expression text editor to find and replace the new email address with the old, but the tool could not accomplish the replacement.

(U//~~FOUO~~) \_\_\_\_\_ used the email address \_\_\_\_\_@gmail.com as an account to test email flow when he worked on the Server. It was a "dummy" account he used to test email issues for various PRN clients.

(U//~~FOUO~~) After reviewing work tickets from July 29-30, 2014, \_\_\_\_\_ stated the ScreenConnect remote sessions with MILLS and HEATHER SAMUELSON were for the purpose of transferring copies of the July Export to their Windows workstations. Prior to the transfer, \_\_\_\_\_ password-protected the .pst, then placed it in an Advanced Encryption Standard (AES) zip file. The ScreenConnect tunnel was also encrypted, resulting in three layers of protection.

(U//~~FOUO~~) After reviewing an invoice dated August 12, 2014, \_\_\_\_\_ stated he assisted SAMUELSON in reconnecting to the July Export archive.

(U//~~FOUO~~) After reviewing a work ticket dated September 29, 2014 and invoices dated September 30, 2014 and October 1, 2014, \_\_\_\_\_ stated he spoke with MILLS about the creation of a new email archive export (September Export). \_\_\_\_\_ could not recall if the September Export consisted of the complete live mailbox belonging to CLINTON, the exported emails from the HRC

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 3  
Archive mailbox, or both. The September Export was several gigabytes in size. \_\_\_\_\_ did not place any limitations or delete any content from the September Export.

b6  
b7C

(U//~~FOUO~~) After reviewing a work ticket dated November 18, 2014, \_\_\_\_\_ stated he worked with SAMUELSON to reestablish her connection to an archive of CLINTON's emails. \_\_\_\_\_ could not recall if it was to the July Export, the September Export, the live HRC Archive mailbox, or something else.

b6  
b7C

(U//~~FOUO~~) After reviewing a work ticket dated November 24, 2014 and an email dated the same day, \_\_\_\_\_ stated he participated in an urgent call with SAMUELSON regarding more specific export requirements. He could not recall the details of the conversation.

b6  
b7C

(U//~~FOUO~~) After reviewing an administrative server log file from November 24, 2014, \_\_\_\_\_ explained he used Microsoft Outlook on the administrative server to test any .pst file exports he created for CESC. The testing consisted of opening the .pst files to ensure they loaded into Outlook correctly.

- Regarding Outlook Office Alert event log entries indicating a mailbox and a "gov export" folder were deleted, \_\_\_\_\_ speculated they were deleted because they were no longer needed on the administrative server.
- Regarding the log entry referencing "huma-gmail-yahoo.pst.lnk," \_\_\_\_\_ stated HUMA ABEDIN requested her email from Gmail and Yahoo be imported into her mailbox on the Microsoft Exchange server. \_\_\_\_\_ could not recall when ABEDIN requested this assistance.

b6  
b7C

(U//~~FOUO~~) After reviewing a document where "HRC Archive" is referenced in the Windows Messaging Subsystem profile for \_\_\_\_\_tmp, \_\_\_\_\_ stated he believed this file to be a reference related to the transfer of email from the Macbook he received from HANLEY described above. Specifically, \_\_\_\_\_ believed he used the Gmail account \_\_\_\_\_@gmail.com to effect the transfer to the HRC Archive mailbox. He might have used the Macbook for this process, but probably used the Server.

b6  
b7C

(U//~~FOUO~~) After reviewing emails dated December 10, 2014 and December 12, 2014, as well as work tickets regarding December 9-10, 2014 telephone calls with MILLS and SAMUELSON, \_\_\_\_\_ stated they wanted the last 60 days of email for CLINTON and ABEDIN in new accounts that were not on the Microsoft Exchange server, but did not request the migration of any other content.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated December 11, 2014 with the subject line "RE: 2 items for IT support," and a December 12, 2014 work ticket referencing email retention changes and archive/email cleanup, \_\_\_\_\_ stated his reference in the email to "...the Hilary [sic] coverup [sic]"

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 4

operation..." was probably due to the recently requested change to a 60 day email retention policy and the comment was a joke. He did not recall the prior retention policy.

b6  
b7C

(U//~~FOUO~~) After reviewing a work ticket dated January 5, 2015, referencing a remote session with MILLS and SAMUELSON, \_\_\_\_\_ stated the session was possibly to remove the July Export or September Export .pst files from their workstations.

b6  
b7C

(U//~~FOUO~~) After reviewing a Server log entry from January, 5, 2015, noting the installation of Ontrack PowerControls (PowerControls), \_\_\_\_\_ stated PowerControls was the software utility bundled with the Datto backup device employed as part of the CESC Server architecture. It is used for Microsoft Exchange server restoration, but \_\_\_\_\_ did not recall ever taking any actions with it.

b6  
b7C

(U//~~FOUO~~) After reviewing a document identifying the "Last Written Time" as January 6, 2015 for "HRC .gov email Archive.pst, HRC .gov emails.pst, HRC gov emails.pst, and export.pst," \_\_\_\_\_ stated Outlook updates the modification time and date for any .pst files attached to a mail account when the program is opened.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated January 7, 2015 containing a list of mailboxes on the CESC server, \_\_\_\_\_ stated he believed the HRC Archive mailbox should still be on the Server in the possession of the FBI. He did not know why it would not be on the server and said he would check the current server for the existence of an HRC Archive mailbox. Users could control the content of a mailbox, but not the existence of it. Only \_\_\_\_\_ and \_\_\_\_\_ had the capability to login to the Server as an administrator and remove a mailbox. \_\_\_\_\_ stated he did not remove the mailbox, nor did anyone request he remove the mailbox.

b6  
b7C

(U//~~FOUO~~) After reviewing administrative server log entries ranging from January to October 2015, referencing multiple Google Apps, \_\_\_\_\_ stated the office of \_\_\_\_\_ used Google Apps for business, so he used Google migration tools to pull the email accounts of users from her office to the Microsoft Exchange server. January 2015, however, was not the correct timeframe for that migration and \_\_\_\_\_ did not recall what he might have used Google Apps for in January 2015.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated March 5, 2015, referencing \_\_\_\_\_ from Security Pursuit, \_\_\_\_\_ stated he did not know \_\_\_\_\_ and did not recall implementing any new security features during that timeframe.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated March 3, 2015, referencing a .pst file containing all of "HRC's emails to/from any .gov addresses," \_\_\_\_\_ stated he used filters based on sending and receiving email addresses, as well as a date filter for CLINTON's time as Secretary of State to produce the July Export.

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 5

(U//~~FOUO~~) After reviewing an email dated March 5, 2015 with the subject line "RE: Share," \_\_\_\_\_ stated the shared drive was located on PRN hardware in Denver. It was a limited access shared drive for individuals working with CESC.

(U//~~FOUO~~) After reviewing an email dated March 5, 2015 with the subject line "RE: CESC Firewall," \_\_\_\_\_ stated "...HRC's backup device..." referred to a second mobile device that belonged to CLINTON. He did not recall any details about the device.

(U//~~FOUO~~) After reviewing a document with information concerning "export.pst, HRC archive – complete.pst, and hrcarchive@clintonemail.com – HRC archive.ost," \_\_\_\_\_ stated, based on the Last Written Time in the registry, that export.pst existed on the administrative server as of March 7, 2015. He did not recall when it was removed or who removed it from the administrative server.

(U//~~FOUO~~) After reviewing work tickets from March 7-8, 2015 \_\_\_\_\_ stated he determined the Cisco Network Attached Storage device brought to the Equinix data center when PRN took possession of CESC's predecessor server and associated equipment did not contain any email content. PAGLIANO had used it for extra storage and it only contained BlackBerry server logs. \_\_\_\_\_ did not know what was on the external USB hard drive that was also part of the predecessor server architecture. PRN did not use either device as part of the Server architecture they designed and implemented.

(U//~~FOUO~~) After reviewing an email dated March 9, 2015 with the subject line "Re: Email/Data Systems," where \_\_\_\_\_ is listed as one of the recipients, \_\_\_\_\_ stated he did not recall seeing the preservation documentation from DAVID KENDALL referenced in the email.

(U//~~FOUO~~) After reviewing work tickets dated March 10, 2015 and March 12, 2015, referencing the movement of email for MILLS, \_\_\_\_\_ stated MILLS did not have an account on the Server and he could not recall what work he might have done for MILLS. MILLS occasionally contacted \_\_\_\_\_ with problems related to her personal email account, so the work tickets may have been of that nature.

(U//~~FOUO~~) After reviewing an email dated March 25, 2015 with the subject line "CESC call," \_\_\_\_\_ stated he had no recollection of the call or what it was about. \_\_\_\_\_ then reviewed an email dated March 25, 2015 with the subject line "Clintons" and a work ticket dated March 31, 2015 referencing a conference call with KENDALL and MILLS. At this point in the interview, \_\_\_\_\_ PRN's counsel, advised \_\_\_\_\_ not to answer any questions related to conversations with KENDALL based on \_\_\_\_\_ protections under the Fifth Amendment.

(U//~~FOUO~~) After reviewing log files dated March 31, 2015, referencing multiple manual deletions from the Datto server used to backup the Server, \_\_\_\_\_ stated he did not recall

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 6

performing the deletions, nor did he recall being asked to delete backups from the Datto server.

\_\_\_\_\_ further stated everyone at PRN has access to the Datto client portal, which is used to manage the backups for all of PRN's clients who employ Datto's services.

(U//~~FOUO~~) After reviewing log files dated March 31, 2015, referencing the installation of BleachBit on the administrative server, \_\_\_\_\_ stated he believed he used the program for the removal of .pst files related to the various exports of CLINTON's email discussed above from the administrative server. He took this action of his own accord based on his normal practices as an engineer. He did not recall which settings he used, to include the overwrite free space feature. \_\_\_\_\_ later stated he might have used BleachBit on the Microsoft Exchange server because any .pst exports would be created there, then moved over to the administrative server and opened to verify the exported .pst file worked correctly.

(U//~~FOUO~~) \_\_\_\_\_ does not recall who or when the conversation occurred, but someone from CESC told him at some point s/he did not want the .pst files hanging around and wanted them off of the Server after the export.

(U//~~FOUO~~) After reviewing a text document with the first line "June of 2013," \_\_\_\_\_ stated he did not recall creating the document. However, the statement "PST Files were shredded" is probably a reference to his use of BleachBit.

(U//~~FOUO~~) After reviewing log files from the administrative server dated January – October 2015, \_\_\_\_\_ stated the reference to Google Apps Sync on April 4, 2015 was possibly an automatic update to the software.

(U//~~FOUO~~) After reviewing an email dated April 24, 2015 with the subject line "4/27-5/1," \_\_\_\_\_ stated the entry on April 27, 2015 was a calendar appointment related to regular maintenance of the Server and associated equipment.

(U//~~FOUO~~) After reviewing an email dated August 18, 2015 with the subject "RE: email," \_\_\_\_\_ stated CESC wanted to verify they had a 60 day retention policy. He believed \_\_\_\_\_ misspoke when \_\_\_\_\_ commented on a 30 day retention policy.

(U//~~FOUO~~) After reviewing an email dated August 21, 2015 with the subject line "RE: Datto remote access," and an email dated August 20, 2015 with the subject line "RE: CESC Datto," \_\_\_\_\_ stated PRN might have received a new Datto server because in the initial setup of the original Datto server, it auto synced with the Datto data center and created an offsite copy. The new Datto server would not allow that to happen.



Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 7

b6  
b7C

(U//~~FOUO~~) After reviewing logs dated September 21-September 26, 2015 from the Microsoft Exchange server and September 25-October 2, 2015 from the administrative server, \_\_\_\_\_ speculated he may have removed mailboxes attached to Outlook on the administrative server. He was not instructed to delete any user mailboxes on the Microsoft Exchange server in September 2015, nor did he delete any mailboxes. Furthermore, \_\_\_\_\_ did not do any work with any email exports in the September 2015 timeframe. It was standard practice for \_\_\_\_\_ to install OnTrack PowerControls on a server because it is required to restore a system from a Datto backup. Additionally, \_\_\_\_\_ would login to the Datto server during regular maintenance appointments to check the backups. Regarding the October visits to the CESC Datto Control Panel referenced in the logs, \_\_\_\_\_ or \_\_\_\_\_ probably logged into the Datto server using ScreenConnect to verify it was running properly. ScreenConnect was \_\_\_\_\_ primary method of connecting to the administrative server.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ did not recall manually running a disk defragmenting utility, but would sometimes do it as part of routine maintenance.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was shown several other documents for which he had no information. All documents used during the interview are attached to this communication as a 1A.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/04/2016

(U//~~FOUO~~) On May 3, 2016, [ ] Platte River Networks (PRN), date of birth [ ] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [ ] and SA [ ] at the United States Attorney's Office for the Eastern District of Virginia located at 2100 Jamieson Avenue, Alexandria, VA 22314. Also present for the interview were Supervisory Special Agent [ ] Information Technology Specialist/Forensic Examiner [ ] Department of Justice (DOJ) Attorney [ ] DOJ Attorney [ ] EDVA Attorney [ ] and EDVA Attorney [ ] as well as [ ] counsel, [ ] and [ ]. After being advised of the identity of the interviewing agents and the nature of the interview, [ ] provided the following:

b6  
b7C

(U//~~FOUO~~) In February 2014, [ ] worked with MONICA HANLEY to import an archive of HILLARY CLINTON's email from an Apple MacBook to the PRN-maintained server hosted for the CLINTON EXECUTIVE SERVICES CORPORATION (CESC). This server hosted CLINTON's email account. HANLEY told [ ] the MacBook contained old email that only existed on the laptop and HANLEY did not want to lose it. The email was stored in Mac Mail within folders labeled by year as 2009 Inbox, 2009 Sent Items, 2010 Inbox, 2010 Sent Items, etc. [ ] tried to effect the transfer of the archived email through a remote session using ScreenConnect, but the WiFi connection was intermittent and the MacBook repeatedly turned itself off. Therefore, HANLEY shipped the MacBook to [ ] was unaware of a USB flash drive containing an identical set of the email files.

b6  
b7C

(U//~~FOUO~~) [ ] tried various tools and Googled for solutions to effectively transfer the email files. After researching options, [ ] transferred all of the email content to the "dummy" gmail account [ ]@gmail.com. [ ] connected the administrative server to the gmail account and used it as a bridge to move the email into a mailbox named hrcarchive on the Exchange server. The PRN architecture consisted of a BlackBerry Enterprise server, domain controller, administrative server, and Microsoft Exchange server (PRN server). After the transfer was complete, he deleted the content from the gmail account and provided the hrcarchive login credentials to HANLEY or [ ] and demonstrated how to access the mailbox using Outlook Web Access. [ ] did not know if [ ] or HANLEY provided the credentials to others; however, anyone with the credentials could access the account. Prior to shipping back the MacBook, either

b6  
b7CInvestigation on 05/03/2016 at Alexandria, VAFile # [ ] 302 Date dictated N/Ab3  
b7EBy SA [ ] SA [ ]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of [redacted] Interview of [redacted], On 05/03/2016, Page 2  
HANLEY or [redacted] requested the email be deleted from the MacBook. [redacted] deleted the files containing the email, but did not use any special tools to remove the files. [redacted] provided an address for the return shipment of the MacBook and [redacted] used either the United States Postal Service or United Parcel Service.

b6  
b7Cb6  
b7C

(U//~~FOUO~~) [redacted]  
and [redacted] all had access to the prnadmin account credentials to access the PRN server. The [redacted] account on the server maintained by BRYAN PAGLIANO was created by PAGLIANO during the transition to the PRN server. There was also a built-in administrator account on the PRN server, but [redacted] never used it. [redacted] handled most day-to-day work tickets for CLINTON's account, while [redacted] handled the physical infrastructure setup and maintenance. [redacted] was authorized to work on the account and served as a backup to [redacted] and [redacted] however, he only handled a few work tickets. [redacted] left PRN in June or July 2015 and, based on PRN's normal business practice, passwords were changed for all admin accounts.

b6  
b7C

(U//~~FOUO~~) In July 2014, CHERYL MILLS emailed [redacted] to schedule a phone call. On the call, MILLS outlined to [redacted] she needed an export of all CLINTON's email sent to or received from a .gov email address (July Export) for the purpose of providing them to the United States Department of State (State). [redacted] searched "\*.gov" in the live "H" mailbox to find email responsive to MILLS' request. After preparing the export, [redacted] worked with MILLS and HEATHER SAMUELSON to transfer the export to each of their workstations. This interaction was the first with MILLS. [redacted] previously interacted with [redacted] and [redacted] MILLS served as the primary contact from which [redacted] took direction for this export and later exports. [redacted] only interacted with SAMUELSON once or twice beyond troubleshooting her access to the exports. He described MILLS and SAMUELSON as proficient computer users with knowledge of basic programs.

b6  
b7C

(U//~~FOUO~~) Based on the direction provided by MILLS as described above, [redacted] prepared an export of CLINTON's email from her live account on the PRN server. [redacted] then used 7-Zip to compress the export and password-protect it. To transfer the export to MILLS and SAMUELSON, he connected to each of their workstations remotely using ScreenConnect and installed 7-Zip. On SAMUELSON's laptop he also installed Outlook 2013 because she did not have Outlook at that time. After the installation of 7-Zip on both workstations and Outlook 2013 on SAMUELSON's workstation, [redacted] transferred the zip file using Secure File Transfer Protocol (SFTP), unzipped the export, and opened the export in Outlook by navigating to it using File->Open->Outlook Data File. When transferring the file, [redacted] likely dropped it on the desktop or in a folder on the C: drive.

b6  
b7C

(U//~~FOUO~~) In September 2014, MILLS contacted [redacted] and requested an export of CLINTON's entire mailbox (September Export), so [redacted] followed a similar process to the July Export. He prepared a .pst file, zipped it using 7-Zip, and transferred it to MILLS and SAMUELSON

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 05/03/2016, Page 3  
 through ScreenConnect. In the preparation of this export, \_\_\_\_\_ discussed different options for the transfer based on the size of the file, but ultimately decided on the same process using ScreenConnect as the July Export. MILLS never requested assistance from \_\_\_\_\_ in locating CLINTON's email from January 2009 – March 2009 and \_\_\_\_\_ was never aware there was a gap during that timeframe.

b6  
b7Cb6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ did not know why the .pst file provided to the FBI from CLINTON's counsel contained the email address \_\_\_\_\_@gmail.com in the metadata because he believed he created email exports from CLINTON's live email mailbox. However, he provided the following possible explanations:

b6  
b7C

- \_\_\_\_\_ may have imported HRC Archive into CLINTON's live mailbox.
- A user may have moved email from HRC Archive into CLINTON's live mailbox.
- A user may have taken email directly from the HRC Archive mailbox to produce what was provided to State. \_\_\_\_\_ did not assist in the production of any .pst files provided to State.

b6  
b7C

(U//~~FOUO~~) During the July Export and September Export, \_\_\_\_\_ transferred one .pst file, contained within a zip file, to MILLS and one to SAMUELSON. Their laptops were running either Windows 7 or Windows 8.

b6  
b7C

(U//~~FOUO~~) After reviewing a chart labeled "PST files and Outlook Profiles – Admin Server," \_\_\_\_\_ stated "HRC .gov email Archive.pst," "HRC .gov emails.pst," and "HRC gov emails.pst" reference the July Exports. \_\_\_\_\_ described the other files as:

b6  
b7C

- "HRC archive – complete.pst" references the September Export.
- "hrcarchive@clintonemail.com - HRC archive.ost" is a remnant of the transfer of files from the HANLEY laptop described above to gmail.
- \_\_\_\_\_@gmail.com - \_\_\_\_\_ temp.pst" \_\_\_\_\_ could not recall creating this .pst file.
- "huma-gmail-yahoo.pst" was a result of \_\_\_\_\_ importing HUMA ABEDIN's email from those services to the PRN server.

b6  
b7C

(U//~~FOUO~~) After reviewing a PRN invoice referencing an October 1, 2014 call with MILLS, \_\_\_\_\_ stated the call was in relation to one of the .pst file transfers.

b6  
b7C

(U//~~FOUO~~) After reviewing a PRN work ticket dated November 18, 2014 referencing a call with SAMUELSON, \_\_\_\_\_ stated he worked with SAMUELSON to reconnect her to CLINTON's email archive.

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 05/03/2016, Page 4

(U//~~FOUO~~) After reviewing an email dated November 24, 2014 with the subject line "MMM," \_\_\_\_\_ stated he did not know what the reference to an urgent call was about.

(U//~~FOUO~~) After reviewing a work ticket dated November 24, 2014 referencing "more specific export requirements," \_\_\_\_\_ stated he did not know what the more specific export requirements were, but did not believe an additional .pst file was transferred. Neither SAMUELSON nor MILLS requested \_\_\_\_\_ assist with searches for emails to/from specific users, emails to/from specific domains, or create additional exports beyond the July and September Exports.

(U//~~FOUO~~) In November or December 2014, MILLS told \_\_\_\_\_ she did not want the exported data on the laptops anymore and requested he securely delete the .pst files previously transferred to MILLS' and SAMUELSON's workstations, but did not specifically request \_\_\_\_\_ use deletion software. Based on the request of MILLS, \_\_\_\_\_ recommended BleachBit, a tool he had used previously with clients who had financial information on computer equipment being decommissioned. \_\_\_\_\_ described BleachBit as a utility that securely deletes files by overwriting data multiple times. He could not recall what version he used, but would have downloaded the latest version at the time of MILLS' request. Sometime prior to this discussion, MILLS mentioned once CLINTON's emails were printed for State, she could put the .pst file on a flash drive and have a master copy. \_\_\_\_\_ had the impression MILLS was referring to all of CLINTON's emails, not just those provided to State.

(U//~~FOUO~~) \_\_\_\_\_ used the same deletion process for the workstations of both MILLS and SAMUELSON. He initiated a remote session, typically while on the phone with MILLS or SAMUELSON, to each workstation using ScreenConnect and downloaded BleachBit from the Internet, then installed the software. He used BleachBit to remove the .pst files by running the shredding function as a standard user, not an administrator. The process took a few minutes to complete during which \_\_\_\_\_ did not encounter an error message. \_\_\_\_\_ believed he shredded a total of eight files – the two zip and two .pst files on each laptop from the July and September exports. He did not recall:

- Altering any settings prior to shredding the .pst files
- Wiping free space
- Selecting artifact clean up
- Verifying the deletion of the files
- Selecting "Shred Settings and Quit" once the process was complete
- Targeting any temporary files
- Uninstalling BleachBit

(U//~~FOUO~~) After reviewing work tickets dated December 12, 2014 and January 5, 2015, \_\_\_\_\_ stated the work tickets reflected the tasks he completed to remove .pst files from the PRN

Continuation of FD-302 of Interview of [REDACTED], On 05/03/2016, Page 5  
server and the workstations of MILLS and SAMUELSON. The requests from MILLS were routine customer service, so no one else at PRN was aware of the removal tasks [REDACTED] completed beyond what was written in the work tickets. Since completion, neither MILLS nor anyone else from CESC contacted [REDACTED] to verify this work was complete. Additionally, [REDACTED] was not contacted by anyone to discuss the process he used to remove the files from the workstations.

(U//~~FOUO~~) In March 2015, MILLS contacted [REDACTED] to discuss CLINTON's email. Typically, MILLS would contact [REDACTED] using the email address [REDACTED]@gmail.com and setup a time to call. MILLS wanted to know what backups of CLINTON's email existed and where those backups were located. After discussing the potential for content to exist on the server CLINTON used prior to the PRN server, PRN decided [REDACTED] would travel to the datacenter in Secaucus, NJ to power up the old equipment (Predecessor server) and check it for any backups or copies of CLINTON's mailbox. After [REDACTED] arrived at the datacenter and turned on the old equipment, [REDACTED] spoke with [REDACTED] while they both were logged on to the system. Neither the Cisco Network Attached Storage (NAS) device nor the external USB hard drive that were part of the architecture for the Predecessor server contained backups or other data associated with CLINTON's email.

(U//~~FOUO~~) PRN used a Datto backup appliance to backup the PRN server and it was PRN's common practice to include the administrative server as part of the Datto backup, but [REDACTED] could not specifically recall if the administrative server was backed up for CESC. [REDACTED] had no memory of stopping Datto backups of the PRN administrative server on March 8, 2015. Datto recommends turning off Windows Volume Shadow Copy service because it can interfere with Datto backups.

(U//~~FOUO~~) [REDACTED]  
[REDACTED]

(U//~~FOUO~~) After reviewing an email dated March 25, 2015 with the subject line "CESC call" and an email dated March 25, 2015 with the subject line "Clintons [sic]," [REDACTED] stated he could not recall the content of the call or the reference to backups in the email.

(U//~~FOUO~~) After reviewing a document titled "Exchange Audit Logs" dated March 25, 2015 and March 31, 2015, [REDACTED] stated the Platte Admin mailbox received firewall alerts and other internal system alerts. Additionally, the Platte Admin account was used to effect changes on other mailboxes. [REDACTED] did not specifically recall using it to provide full access for prnadmin to the mailboxes H, HDR29, and HRC Archive on March 25, 2015 and then removing the HRC Archive mailbox from the Exchange server. However, [REDACTED] believed he had an "oh shit" moment and removed the HRC Archive mailbox. He also changed the mailbox retention policy from 30 days to 1 day, and cleaned the mailbox database because MILLS previously requested in late 2014 or early 2015 he change the retention policy for CLINTON and ABEDIN's existing and ongoing email to 60 days. He removed the HRC

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 05/03/2016, Page 6

Archive mailbox manually because all content in the mailbox was older than 60 days. \_\_\_\_\_ changed the deleted items retention policy from 30 days to 1 day to ensure no email outside of the 60 days remained on the server and executed the Clean-MailboxDatabase command to clean whitespace within the database, similar to running a disk defragmentation. \_\_\_\_\_ also enabled Circular Logging, but did not recall why he did so in this instance. He typically enabled it when importing email because Microsoft Exchange logs contain email that hasn't been committed to a database. Circular Logging reduces the log file size by forcing Exchange to commit data to the database immediately.

b6  
b7C

(U//~~FOUO~~) After reviewing documents titled "BleachBit – PRN Admin Server" and "BleachBit – Exchange Server" indicating the use of BleachBit on March 31, 2015, \_\_\_\_\_ stated he checked the Exchange Server for remaining copies of CLINTON's email. When he located a .pst file, he used the most recent non-beta version of BleachBit available at the time to shred the .pst files on the PRN server, but did not recall which .pst files he found or removed. He did not wipe free space, encountered no errors, and viewed the folders to see if the files were gone, but did not take additional steps to confirm the deletions. \_\_\_\_\_ did not talk with MILLS about the files he found and deleted.

b6  
b7C

(U//~~FOUO~~) After reviewing log files dated March 31, 2015 indicating the deletion of files from the Datto backup appliance, \_\_\_\_\_ stated he did not recall deleting any Datto backups nor did he recall receiving an instruction to delete backups from the Datto, however, it is unlikely anyone else at PRN would have deleted the files. \_\_\_\_\_ did not know if the administrative server was backed up to the Datto.

b6  
b7C

(U//~~FOUO~~) After reviewing a document titled "PRN Admin Server – Installed/Uninstalled Application Events," \_\_\_\_\_ stated he had no insight into the installation of Google Apps Sync for Microsoft Outlook on April 5, 2015.

b6  
b7C

(U//~~FOUO~~) After reviewing documents titled "Add-MailboxPermission and Remove-MailboxPermission" and "Export.pst on Admin Server – 9/25/2016 [sic]," \_\_\_\_\_ stated in September 2015 he looked into replacement options for the PRN server because he believed the server would be turned over to the FBI. To prepare for this eventuality, he logged onto the server to verify the backups of the server were working correctly and evaluate what new hardware PRN would need to order. During the same time frame, \_\_\_\_\_ restored the mailbox for \_\_\_\_\_. This restoration may account for the activity related to Export.pst in September 2015 and it is unlikely Export.pst contained any of CLINTON's email. \_\_\_\_\_ deleted \_\_\_\_\_ Export.pst after the restoration was complete. However, he did not delete any data related to CLINTON's email after he was interviewed by the FBI in September 2015.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated March 9, 2015 referencing a preservation email from DAVID KENDALL and a preservation request from the FBI dated July 31, 2015, \_\_\_\_\_ stated he was aware of the preservation requests and interpreted both as meaning he should not disturb CLINTON's

b6  
b7C

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 05/03/2016, Page 7  
email data on the PRN server. \_\_\_\_\_ did not receive guidance from other PRN personnel or PRN  
counsel, or others regarding the meaning of either preservation request.

b6  
b7Cb6  
b7C



-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/14/2015

On September 11, 2015, [redacted]  
[redacted] United States Department of State (DoS), 2201 C Street NW, Washington, D.C. 20520,  
office telephone [redacted] was interviewed by FBI Special [redacted] and [redacted]  
[redacted] Also present was [redacted] DoS,  
office telephone [redacted] After being advised of the identity of the interviewing agents and the  
nature of the interview [redacted] provided the following information:

b6  
b7C

Principal Officer Electronic Messaging System (POEMS) was a Top Secret DoS email system that was phased out several years ago. Today the term POEMS is often used by people referring to the DoS email systems provided by the Office of the Secretary, Office of the Executive Secretariat - Information Resource Management (S/ES-IRM). While the majority of DoS employees receive IT support from Information Resource Management (IRM), a subset of approximately 600 individuals receive IT support from S/ES-IRM. This subset is composed of high-level DoS executives and staff, who are collectively referred to as the "7<sup>th</sup> floor." The S/ES-IRM system was created to provide the 7<sup>th</sup> floor users with enhanced customer service.

Despite being administered by separate groups, the IRM and S/ES-IRM systems utilize the same hardware and software platforms. Both groups support their respective users across both Opennet, the unclassified DoS network, and Classnet, the classified DoS network. The top secret network at DoS is operated by the Bureau of Intelligence and Research (INR) regardless of the user.

S/ES-IRM does not have stand-alone email backup. Historical emails have to be extracted from an overall system backup. The volume of available historical emails therefore depends on what each user had saved on their system when the system backup occurred. The entire S/ES-IRM system is backed up every night during which the email exchange, as well as file servers, shared drives, applications and other relevant files are captured. The backup tapes are held for 45 days. S/ES-IRM has pulled the relevant S/ES-IRM system backup tapes in response to the preservation requests issued by the FBI and is preserving them until they receive further direction from the FBI. [redacted] estimated that approximately 100 of the 600 S/ES-IRM customers were listed on the preservation request.

b6  
b7C

[redacted] provided that the exchange servers are housed at ESOC in Culpeper, VA and that the backups are stored at the Harry S. Truman building.

b6  
b7C

---

Investigation on 09/11/2015 at Washington, DCFile # [redacted] Date dictated N/Ab3  
b7EBy SA [redacted]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 09/14/2015, Page 2b6  
b7c

S/ES-IRM customers do not use the State Messaging and Archival Retrieval Tool (SMART) for memorializing official email records. Instead, they follow the "print and file" policy whereby each individual is responsible for assessing if a communication should be archived and is then responsible for printing and appropriately filing the communication. SMART is primarily used for archiving cable traffic and replaced a legacy system known as CableXpress approximately four or five years ago.

S/ES-IRM does not administer the Public Affairs Communication Electronically (PACE) system, which is operated by the Bureau of Diplomacy. PACE is a much smaller system but it is possible that a few people from Secretary Clinton's staff may have used PACE.

DoS does not have a restriction on the use of personal email accounts for official business. Personal email accounts are often used by individuals in the field who were not issued an official DoS mobile device, or who do not have the time or means to remotely log into the DoS system. Employees are not required to notify DoS that they are using a personal account for official business and there is no mechanism to track who is using a personal email account. In 2009 and 2014, DoS issued official guidance to users of personal email accounts that stipulated that they must forward work-related emails back to their official work account within a specified period of time for record keeping purposes.

S/ES-IRM does not automatically create Opennet or Classnet email accounts for new employees. Accounts are only created once a request form has been submitted. S/ES-IRM had no record of a request being completed by, or on behalf of, Secretary Clinton for the creation of DoS email accounts. Nor were there any records of requests being made for a DoS mobile device.

S/ES-IRM is also responsible for issuing official cell phones and other mobile devices to their 7<sup>th</sup> floor customers. However, S/ES-IRM does not have historical records for devices issued during Secretary Clinton's tenure. The system that was used for tracking property during that time period was previously taken offline and S/ES-IRM has been unable to restore the system due to the presence of corrupt files. While users were required to sign a property record when a device was issued to them, those records would have been destroyed once the device was returned to S/ES-IRM.

[REDACTED] was not able to provide any specific information about the broader IRM system and their efforts to preserve relevant data. He recommended contacting [REDACTED] via the Bureau of Diplomatic Security (DS) [REDACTED]. [REDACTED] noted that BRIAN PAGLIANO works for [REDACTED] and care should be taken when contacting IRM.

b6  
b7c

[REDACTED] and [REDACTED] were available for future contact if necessary.

b6  
b7c

♦♦

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/14/2016

(U//~~FOUO~~) On January 11, 2016, MONICA HANLEY was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at [redacted] Washington, DC 20001. Representing HANLEY, and also present for the interview, were [redacted] and [redacted]. After being advised of the identities of the interviewing agents, and the purpose of the interview, HANLEY provided the following information:

b6  
b7C

(U//~~FOUO~~) In 2003, following her college graduation, HANLEY interned for then Senator HILLARY CLINTON. HANLEY's internship position was converted to a permanent position in 2004. HANLEY continued working for New York Senator KIRSTEN GILLIBRAND, who was appointed after CLINTON was nominated as Secretary of State.

(U//~~FOUO~~) In April of 2009, HANLEY received a call from HUMA ABEDIN asking if HANLEY would be interested in working for CLINTON as a "Confidential Assistant" at the Department of State (DoS). HANLEY accepted the position at DoS, and continued working for GILLIBRAND until two days before her start at DoS.

(U//~~FOUO~~) During her first year at DoS, HANLEY's "Confidential Assistant" duties included supporting and scheduling CLINTON, domestic travel and personal appointments. HANLEY also ran various errands for CLINTON. HANLEY also served as ABEDIN and JAKE SULLIVAN's scheduler, and it was her responsibility to coordinate their schedules with CLINTON's schedule.

(U//~~FOUO~~) HANLEY accompanied CLINTON on foreign travel on a few occasions during her first year at DoS. HANLEY's first overseas DoS travel with CLINTON was to the Philippines. CLINTON specifically invited HANLEY to join her on that trip because CLINTON knew HANLEY was of Filipino decent and would appreciate the opportunity to travel there. ABEDIN almost always traveled with CLINTON. [redacted] and [redacted] were additional aids who rotated duties with HANLEY in regards to accompanying CLINTON on foreign travel.

b6  
b7C

(U//~~FOUO~~) When ABEDIN became pregnant in 2011, HANLEY became a primary traveler and accompanied CLINTON on most of her foreign trips. [redacted] and [redacted] were also part of CLINTON's travel team during this time. [redacted] was responsible for managing press matters, whereas [redacted] were responsible for protocol.

b6  
b7C

Investigation on 1/11/2016 at Washington, D.C.

File # [redacted]-302 Date dictated N/A

By SA [redacted] SA [redacted]

b3  
b7E

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~SECRET~~

Continuation of FD-302 of Interview of Monica Hanley, On 1/11/2016, Page 2

(U//~~FOUO~~) HANLEY went through a full day of on board training her first day at DoS, of which approximately half was security related. HANLEY recalled learning specifically how to handle and transport classified information/paper, but could not recall who provided the training. HANLEY received a Top Secret/SCI clearance at DoS, but was unsure of any specific codeword programs for which she may have additionally received read-ins. HANLEY did not hold a security clearance prior to DoS.

(U//~~FOUO~~) HANLEY did not recall ever receiving Freedom of Information Act (FOIA) training, and the only training HANLEY received concerning the Federal Records Act (FRA) came near the end of CLINTON's tenure at DoS. A representative from DoS's record keeping office, [REDACTED] Last Name Unknown (LNU), met with HANLEY and others on CLINTON's staff and instructed them to produce all records that "changed, effected, or created policy." HANLEY recalled going through paper files with other executive Staff members, and placing the papers in stacks in the hallway outside the Secretary's Suite. After which, a DoS record keeper would review the production and make the final determination on which information was relevant to the FRA.

b6  
b7C

#### Email Accounts and Server

(U//~~FOUO~~) During her time in the Senate, CLINTON used hr15@att.blackberry.net. HANLEY was aware of this email account, but did not use this account to communicate with CLINTON.

(U//~~FOUO~~) CLINTON used hrod17@clintonemail.com while she was Secretary of State, and hdr22@clintonemail.com following her departure from DoS.

(U//~~FOUO~~) HANLEY did not initially recall the account [REDACTED]@gmail.com, however, later in the interview HANLEY deduced the [REDACTED]@gmail.com account may have been created as a way to communicate with CLINTON during a bad storm in 2011 when power to the server hosting hdr22@clintonemail.com was lost. HANLEY believed CLINTON was traveling in Croatia at the time, and HANLEY and [REDACTED] may have created the account as a temporary way to communicate with CLINTON during the outage.

b6  
b7C

(U//~~FOUO~~) HANLEY was not familiar with the email address SSHRC@state.gov. HANLEY vaguely recalled CLINTON being issued a DoS Blackberry, but CLINTON did not use the DoS issued device.

(U//~~FOUO~~) HANLEY was aware CLINTON was using a personal email address on a personal server for DoS business while CLINTON was Secretary of State. JUSTIN COOPER created, installed, and maintained the server in Chappaqua before the server was transitioned over to Platte River Networks (PRN). HANLEY could not recall when the transition to PRN occurred. COOPER was HANLEY's point of contact for assistance in regards to syncing CLINTON's mobile devices to the server. Anytime CLINTON got a new device, HANLEY would contact COOPER who would troubleshoot her through the process of setting up the new device with the server. COOPER was also HANLEY's point of contact

Continuation of FD-302 of Interview of Monica Hanley, On 1/11/2016, Page 3

when needed reimbursment for items she purchased for CLINTON. COOPER was located in New York, so most of HANLEY's interaction with him was via email or telephone.

(U//~~FOUO~~) BRYAN PAGLIANO was part of CLINTON's 2008 Presidential Campaign and was later employed by DoS in a technical capacity. HANLEY would contact PAGLIANO for help with physical Blackberry problems.

(U//~~FOUO~~) HANLEY did not recall ever participating in, or overhearing, any discussion over records retention issues, nor the legality of CLINTON conducting DoS business off a private server or email account.

(U//~~FOUO~~) HANLEY was asked to review a few emails forwarded from CLINTON at hrod17@clintonemail.com to HANLEY's DoS email account wherein CLINTON asks HANLEY to print the forwarded email. After reviewing the email, HANLEY explained CLINTON did not like reading things on her Blackberry because it was difficult to read the small font, so she preferred a hard copy for longer emails. Sometimes CLINTON would keep the hard copy to archive the document, but HANLEY was not privy to what documents CLINTON had printed for an easier read versus archiving.

(U//~~FOUO~~) HANLEY used two email accounts while at DoS: hanleymr@state.gov and [REDACTED]@gmail.com. HANLEY did not have an @clintonemail.com email account, nor was she ever offered an @clintonemail.com account. As a way of general practice, HANLEY tried her best to use her state.gov email account for work related matters and her Gmail account for personal interactions with CLINTON. HANLEY further explained she considered personal interactions with CLINTON to include things like scheduling hair appointments. However, HANLEY noted that her state.gov email account was not as easily accessible as her Gmail account and on some occasions she use Gmail when she could not access her state.gov account.

b6  
b7c

(U//~~FOUO~~) HANLEY was issued and carried/used a DoS Blackberry. It was difficult to access DoS email while on travel, as the DoS system required users to sign in using a token/key to sign in remotely. It was particularly difficult to sign into the DoS system in the Secretary's plane because the wifi was not always compatible, so HANLEY would often use her Gmail account while in the air. The same was true for foreign travel. Many DoS employees used personal email accounts because they were more easily accessible. ABEDIN emailed HANLEY equally from her state.gov and personal accounts.

### Mobile Devices

(U//~~FOUO~~) After she reviewed pictures of various Blackberry models, HANLEY pointed to the picture of the Curve 8310 explained CLINTON preferred the Curve 8310 because she found the 8310 "track-ball" feature easier than the "track-pad" on newer Blackberry models. CLINTON tried the Blackberry 8700G, but did not like the device because of the "track-pad." HANLEY also thought the Curve 8900 looked familiar. HANLEY did not recall the specific Blackberry devices CLINTON used at DoS, but believed CLINTON's original Blackberry was black in color and housed in a blue silicone case.

Continuation of FD-302 of Interview of Monica Hanley, On 1/11/2016, Page 4

(U//~~FOUO~~) HANLEY recalled helping CLINTON change her Blackberry device at least three or four times while she was at DoS. HANLEY recalled having to replace CLINTON's Blackberry on one occasion after CLINTON spilled coffee on the device. Another time HANLEY recalled having to replace CLINTON's Blackberry because it started to slowly fail overtime. HANLEY recalled proactively trying to purchase replacement Blackberrys for CLINTON at one point, but CLINTON only liked the older models. HANLEY believed she may have even purchased one of the older Blackberry models CLINTON liked off of Ebay.

(U//~~FOUO~~) HANLEY would contact COOPER after purchasing a new Blackberry device for CLINTON, and he would instruct HANLEY as to how to connect the device and sync the device with CLINTON's server and email. Once the new device was properly synced, COOPER would also talk HANLEY through the process of wiping the old device. HANLEY would provide the new Blackberry to CLINTON along with the old/wiped Blackberry. However, HANLEY was not sure what CLINTON did with the old Blackberry after HANLEY turned them over.

(U//~~FOUO~~) Aside from receiving emails on her Blackberry, CLINTON used her Blackberry to text and pin short personal messages.

(U//~~FOUO~~) CLINTON also used an iPad. HANLEY could not recall when CLINTON obtained the iPad, but thought it may have been purchased by COOPER. HANLEY was not sure who configured CLINTON's iPad. CLINTON predominately used the iPad in the evenings and while on travel (both domestic and international) for reading news articles and emails. CLINTON did use the iPad to send and receive emails. CLINTON did not use the iPad while she was in her office at DoS.

(U//~~FOUO~~) ABEDIN, HANLEY, and [ ] had access to CLINTON's iPad on occasion to assist CLINTON if her iPad was not working properly, but HANLEY could not recall CLINTON giving her iPad to anybody else to use.

b6  
b7c

(U//~~FOUO~~) CLINTON received a new iPad in 2011 and gave HANLEY an iPad around the same time. HANLEY assumed CLINTON gifted her with CLINTON's old iPad. Agents asked HANLEY to review an email exchange dated 8/18/2011 between ABEDIN and COOPER in which ABEDIN tells COOPER "She [presumably CLINTON] doesn't like ipad 2..." and later typed "She gave to monica as a birthday gift." After reviewing the email, HANLEY explained that she assumed she received CLINTON's old iPad, but now realizes she likely received CLINTON's newer iPad. HANLEY was not aware the iPad was a birthday gift, but stated that it was not uncommon for CLINTON to gift ABEDIN and HANLEY with some of her personal items she no longer wanted.

(U//~~FOUO~~) When HANLEY received the iPad the opening screen said "H's iPad," so before using the gifted iPad, HANLEY wiped the device. HANLEY used the iPad for personal use up until the time she moved back to New York in 2014. Prior to moving, HANLEY gave the iPad to [ ]

b6  
b7c

Continuation of FD-302 of Interview of Monica Hanley, On 1/11/2016, Page 5

[redacted] so he could use the iPad to listen to music and podcasts. HANLEY did not wipe the iPad prior to gifting it to [redacted]

b6  
b7C

(U//~~FOUO~~) In October of 2013, HANLEY received a call from CHERYL MILLS who inquired about the iPad. HANLEY explained she received what she believed was CLINTON's old iPad as a gift from CLINTON in 2011. MILLS subsequently informed HANLEY she needed to turn over the iPad in response to the FBI's investigation. HANLEY contacted [redacted] to retrieve the iPad and turned it over.

b6  
b7C

### Laptop Computer

(U//~~FOUO~~) After they learned longtime friend of CLINTON, SIDNEY BLUMENTHAL, was the target of an email hack in Spring of 2013, PRN spoke with COOPER, ABEDIN, and HANLEY, and advised CLINTON change email addresses. CLINTON did not want to lose her old emails when she changed her email address. COOPER subsequently provided HANLEY an extra Apple Macbook from President Clinton's Harlem, NY, Office. HANLEY then transferred all of CLINTON's old emails from the PRN server to the Macbook Air. HANLEY transferred the emails to the Macbook in her [redacted] apartment, and noted that it took several days because she transferred four years of emails. HANLEY also recalled transferring the emails to a thumb-drive, but could not recall what happened to the thumb-drive.

b6  
b7C

(U//~~FOUO~~) HANLEY maintained possession of the Macbook following the transfer of the emails. The Macbook was stored in HANLEY's apartment. HANLEY moved at least once after she transferred the emails to the Macbook, and brought the Macbook with her to her new apartment.

(U//~~FOUO~~) HANLEY continued to work for CLINTON following DoS, and in early 2014 took a position in the [redacted]. Shortly thereafter, HANLEY realized she still had possession of the Macbook containing CLINTON's archived emails. HANLEY subsequently contacted PRN on her own accord and spoke with [redacted] and [redacted]. HANLEY shipped the Macbook to [redacted] in [redacted] in February and instructed PRN to migrate the emails back to CLINTON's existing server, wipe the Macbook, and return the Macbook to [redacted] who was CLINTON's [redacted] at the time.

b6  
b7C

(U//~~FOUO~~) The Macbook was shipped from [redacted]  
[redacted]

b6  
b7C

(U//~~FOUO~~) When HANLEY was first contacted by FBI agents in November 2015 in regards scheduling an interview, she reached out to [redacted] to ask about the whereabouts of the Macbook. [redacted] told HANLEY she did not recall receiving the Macbook from PRN.

b6  
b7C

Continuation of FD-302 of Interview of Monica Hanley, On 1/11/2016, Page 6**Handling of Classified Material**

(U//~~FOUO~~) CLINTON did not have a classified DoS account, and received all classified information in paper form. CLINTON's Executive Assistant, JOE McMANUS, was responsible for determining what classified information needed to be passed up to CLINTON. The Central Intelligence Agency (CIA) Presidential Daily Briefer (PDB) on occasion may have also flagged information for CLINTON to read. When CLINTON was on travel, her traveling Executive Assistant or SULLIVAN would determine what classified information needed CLINTON's attention.

(U//~~FOUO~~) HANLEY visited both CLINTON's Chappaqua, NY, and Washington, DC, residences, however, HANLEY spent more time in CLINTON's Washington, DC, home. HANLEY believed CLINTON had a Sensitive Information Compartmented Facility (SCIF) installed on [REDACTED] floor of her Chappaqua home that contained at least a secure phone and fax. CLINTON also had a SCIF in her DC home. HANLEY believed the DC SCIF contained a secure phone and unclassified Mac desktop, but was not sure about a fax machine.

b6  
b7c

(U//~~FOUO~~) When the DoS Operations Center needed to get classified material to CLINTON at her DC residence, the information would be couriered by her security detail in a diplomatic pouch. Only a few people close to CLINTON, such as HANLEY could deliver the diplomatic pouch directly to her. HANLEY assumed CLINTON's [REDACTED] in Chappaqua, [REDACTED] could also accept and deliver diplomatic pouches.

b6  
b7c

(U//~~FOUO~~) A DoS Mobile Communications Team (MCT) traveled with CLINTON on both international and domestic trips. The MCT was responsible for setting up a command post for CLINTON's team. Depending on the security climate at the destination, the mobile command post would [REDACTED] b1 per DOS [REDACTED] by CLINTON or her designated staff. The MCT generally set up an unclassified DoS computer in either ABEDIN or HANLEY's room for the purpose of printing unclassified information for CLINTON. It was not uncommon for HANLEY to use her personal Gmail account to print from the mobile DoS unclassified terminal because even though she was using a DoS computer, the DoS connection was unreliable.

(U//~~FOUO~~) CLINTON had a secure phone in her office at DoS, as well as in both her Washington, DC, and Chappaqua, NY, residences. When CLINTON was traveling, ABEDIN would generally carry a secure cell phone. HANLEY carried the secure phone on occasion, and described the phone as looking like an old Nokia non-flip phone with a big antenna and large buttons. The secure cell phone was carried in a box. ABEDIN kept a secure cell phone in her desk at DoS.

(U//~~FOUO~~) HANLEY received a lesson from somebody on the DoS technical team in regards to using the secure cell phone, but when HANLEY tried to use the secure cell phone in 2012 on a trip to Haiti, it did not work.



Continuation of FD-302 of Interview of Monica Hanley, On 1/11/2016, Page 7**Email Review**

(U//~~FOUO~~) HANLEY was contacted by CLINTON's attorney, DAVID KENDALL (Williams & Connolly), in March or April of 2015. Following her conversation with KENDALL, HANLEY searched the Gmail account she used while at DoS for any email communications with state.gov accounts and deleted emails associated with state.gov accounts. HANLEY was not involved with any efforts to review and cull CLINTON's emails.

**General Security Matters**

(U//~~FOUO~~) HANLEY never personally was notified of an intrusion attempt against any of her email accounts (personal or Gmail), however, she remembered hearing some state email accounts were hacked by presumably the Chinese Government following one of CLINTON's trips to China.

(U//~~FOUO~~) HANLEY also received verbal security counseling from Diplomatic Security (DS) following a Russia trip on which she accompanied CLINTON. HANLEY was handed a diplomatic pouch containing CLINTON's briefing book on the plane upon arriving in Russia. HANLEY brought the pouch and its contents into the Russian hotel suite she shared with CLINTON. DS found a classified document from the briefing book in the suite during a sweep following CLINTON and HANLEY's departure, and HANLEY was later informed by DS the briefing book and document should never have been in the suite.

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/13/2015

(U//~~FOUO~~) [redacted] was interviewed at his office at the Harry S. Truman Building, 2201 C Street NW, Washington, D.C., by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and [redacted]. After being advised of the identity of the interviewing agents, and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) In February 2009, [redacted] was assigned as a [redacted] in the Department of State (DoS) Operational Center. DoS's Operational Center is manned 24 hours a day by three different watch shifts. Sometime in 2009, [redacted] became a [redacted] which meant that [redacted]

b6  
b7C

(U//~~FOUO~~) In either March or April of 2010, [redacted] for Secretary of State HILLARY CLINTON. [redacted] CLINTON's [redacted]. Before [redacted] he filled in on a few occasions for his predecessors in the role [redacted] and [redacted] Last Name Unknown (LNU). [redacted] during her tenure as Secretary of State. [redacted] and [redacted] were already in place when CLINTON was appointed.

b6  
b7C

(U//~~FOUO~~) In his role as CLINTON's [redacted] was responsible for reviewing and filtering information intended for CLINTON. [redacted] reviewed various reports and information/action memos to determine which warranted forwarding to CLINTON, and would subsequently filter out and clean up the most relevant information to forward to CLINTON via her Executive Secretary, JOSEPH MACMANUS. The reports [redacted] reviewed were a "mixed bag," and included everything from unclassified ceremony notifications and Talking Points, to Secret and Top Secret intelligence briefings.

b6  
b7C

(U//~~FOUO~~) CLINTON did not have a computer in her office, nor any electronics [redacted] was aware of, so all briefing materials forwarded for CLINTON's review in office were provided in paper form. [redacted] was responsible for making sure he properly organized and marked the reports he forwarded in regards to their classification.

b6  
b7C

---

Investigation on 11/13/2015 at Washington, D.C.b3  
b7EFile # [redacted]-302 Date dictated N/ABy SA [redacted] SA [redacted]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED] On 11/13/2015, Page 2

b6  
b7C

(U//~~FOUO~~) There was no specific guidance as to what information [REDACTED] were expected to forward up to the Secretary's attention. [REDACTED] initially ran things by MACMANUS, but quickly got a sense of what information needed to be pushed up the chain.

b6  
b7C

(U//~~FOUO~~) CLINTON had an Advance Staff of twelve to fifteen people, referred to as "The Line," who would serve as CLINTON's Special Assistants while she was on travel. When CLINTON was traveling, [REDACTED] would communicate with "The Line" and MACMANUS via both unclassified and classified systems. ALICE WELLS eventually replaced MACMANUS as CLINTON's Executive Secretary.

b6  
b7C

(U//~~FOUO~~) [REDACTED] did not recall ever emailing CLINTON directly, and specifically stated that it would have been "weird" for him to send CLINTON an email. The only time [REDACTED] thought he may have emailed CLINTON directly would have been during the Royal Wedding. If [REDACTED] needed to push information up to the Secretary via email, he would reach out to either MACMANUS or her Chief of Staffs, HUMA ABEDIN and JAKE SULLIVAN.

b6  
b7C

(U//~~FOUO~~) [REDACTED] described SULLIVAN as a "work-a-holic," and explained he served in the role as the Deputy Chief of Staff (COS) for Policy. It would not be uncommon for SULLIVAN to work very late at night. ABEDIN served in the role of Deputy COS for Operations, and was more concerned with logistics related to CLINTON's travel.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was unaware that CLINTON was working off of a personal server. [REDACTED] only received a few emails directly from CLINTON, which appeared from "H." [REDACTED] thought it was a little odd because the DoS email naming convention was usually last name, first name, however, [REDACTED] did not recall checking the actual email address. [REDACTED] assumed CLINTON's email was regulated by DoS, as she had a DoS Blackberry.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was assigned to [REDACTED] from 2012-2013, and recalled [REDACTED] being very specific about the process for record emails. [REDACTED] did not remember receiving similar guidance concerning records emails at DoS. Because of the banner information on DoS computer systems, [REDACTED] assumed that all of his DoS emails were for the record.

b6  
b7C

(U//~~FOUO~~) [REDACTED] is a user of the DoS POEMS system. [REDACTED] recalled periodically receiving notification from the systems administrators concerning attempted hacks to the POEMS system. [REDACTED] could not recall the specifics or the timing of these notifications.

b6  
b7C

(U//~~FOUO~~) Interviewing agents asked [REDACTED] to review an email sent from [REDACTED] dated 4/10/201, and titled "Stevens Update (Important)," as publically available online in the DoS Reading Room. The email was addressed to SULLIVAN, ABEDIN, WELLS, and S\_SpecialAssistants [REDACTED]

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED]. On 11/13/2015. Page 3b6  
b7C

stated he was familiar with the email and was aware that it was recently released as part of a recent Freedom of Information Act (FOIA) request concerning CLINTON's emails.

(U//~~FOUO~~) The email in question originated as an unclassified email from the DoS Operations Center to [REDACTED] who stripped the preceding trail of emails and possibly fixed a few grammatical and spelling errors before forwarding the email on to SULLIVAN, ABEDIN, and WELLS. [REDACTED] noted that he likely also added "(Important)" in the Subject line of the email, but did not make any substantive changes to the email before forwarding it. The email would have initially come to [REDACTED] from a specific person in the Operations Center. However, [REDACTED] did not recall who specifically in the Operations Center sent that particular email. [REDACTED] did not have a record of the email he received from the Operations Center, but stated that the Operations Center does maintain all records. MCMANUS and/or [REDACTED] would be individuals with access to the Operations Center records.

b6  
b7C

(U//~~FOUO~~) [REDACTED] did not push forward all information he received from the Operations Center. However, he would orally brief information more often than email. [REDACTED] could not recall an instance where he was concerned with the Operations Center moving classified information from the high side to the low side.

b6  
b7C

(U//~~FOUO~~) The majority of the personnel in the Operations Center are Civil Service employees who receive extensive structured training before they are on their own on the "Ops Floor." The Operations Center receives information from all over the Intelligence Community (IC). One person on each watch shift is tasked with the "watch fax," which receives reports from all over the IC.

(U//~~FOUO~~) [REDACTED] further stated that he thought the "discussion over (the aforementioned) email was healthy, and thinks that there is likely a problem with the way DoS gathers and uses information" from the IC.

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/18/2015

[redacted] Office of Information Programs and Services (IPS), United States Department of State (STATE) Bureau of Administration, [redacted] Washington, D.C. 20520, office telephone [redacted] mobile telephone [redacted] email [redacted]@state.gov, date of birth [redacted] was interviewed in person by FBI Special Agents [redacted] and [redacted] at FBI Headquarters, 935 Pennsylvania Avenue Northwest, Washington, D.C. 20535. After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

[redacted] began working for IPS in [redacted] 2015. Initially, IPS officials were told there were 14 bankers boxes of former Secretary of State Hillary CLINTON's emails at CLINTON's Friendship Heights office. Later, officials were told that the boxes would be picked up from Williams & Connolly, LLP. On or about December 5, 2014, IPS personnel picked up only 12 bankers boxes of CLINTON's emails from Williams & Connolly. [redacted] and other IPS officials were not sure if the boxes were consolidated or what could have happened to the two other boxes. The boxes were labeled with date ranges, which were accurate for the most part. Some of the documents were filed out of order. [redacted] opined the documents were pre-arranged differently than one would expect if the documents were simply printed out and then stacked into the boxes. IPS personnel provided copies of the documents to STATE's Bureau of Legislative Affairs, Office of the Legal Adviser, and the Office of Congressional and Public Affairs.

b6  
b7C

Although, CLINTON was sworn in as Secretary of State in January 2009, IPS officials were unable to locate any of her emails from January-April 2009 in the documents provided by Williams & Connolly. [redacted] did not know whether CLINTON used a different email address at that time. A preliminary review of the documents did not occur until months later. IPS had to wait on the Office of Legal Counsel to provide an official determination as to whether the emails would be considered official STATE records. At some point, the determination was made that the emails would not be considered official STATE records.

b6  
b7C

Based on the dates on the boxes, [redacted] opened the box with the Benghazi-related incidents first. There were sensitive Benghazi-related records, some records related to the National Archives and Records Administration, and some personal emails in that box. [redacted] Records and Archives [redacted] performed the records appraisal. [redacted] informed [redacted] there were some potential classified emails, including some from Sidney BLUMENTHAL, that appeared to have

b6  
b7CInvestigation on 08/17/2015 at Washington, DCFile # [redacted] Date dictated N/Ab3  
b7EBy SA [redacted] SA [redacted]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of [redacted] Interview of [redacted], On 08/17/2015, Page 2

been written by Tyler Drumheller, former Central Intelligence Agency (CIA) Division Chief, European Division. [redacted]

[redacted] as well as other emails that discussed various information related to various foreign governments.

Sometime around late January 2015 [redacted] gave a status brief about the emails to STATE officials Patrick KENNEDY, Under Secretary for Management, [redacted] Bureau of Administration, and [redacted] Global Information Services. KENNEDY and [redacted] were each provided with two binders full of email examples of documents [redacted] believed were possibly classified. [redacted] returned her binders to [redacted] but KENNEDY decided to keep his binders following the brief.

[redacted] was not aware of anyone in IPS or at STATE who received the rules or parameters the CLINTON team and/or Williams & Connolly used to segregate CLINTON's personal and official work emails. There were approximately 60,000 emails, which were reduced to about 30,000. IPS had requested [redacted] Legal Adviser, STATE to ask Williams & Connolly for the rules they used.

To date, [redacted] did not believe [redacted] received a response. [redacted] STATE Inspector General, was also trying to determine how Williams & Connolly performed their review and what basis they used in reducing the emails. Initially, Cheryl MILLS, former CLINTON Counselor and Chief of Staff, was the only CLINTON staff member to respond to a formal request by STATE for information pertaining to personal email and devices used to conduct official STATE business.

According to [redacted] in February 2015, [redacted] attorneys at STATE's Office of Congressional Affairs since approximately [redacted] and [redacted] along with attorneys from the Office of Legislative Affairs, performed their review of the 30,000 emails, from which 296 emails were located and produced responsive to requests from the U.S. House of Representatives Select Committee on Benghazi. The manual paper search was done using keywords "Libya," "Benghazi," and "security."

Prior to the formal EOIA review by IPS of the 296 emails, Congress threatened to release the 296 emails based on [redacted] input that her team had already coordinated with the appropriate STATE bureaus and inter-agency reviewing officials. However, [redacted] and her team did not work with the regular interagency reviewers familiar to [redacted] did not include [redacted] Office of Information Management or [redacted] Records Management Division, FBI. [redacted] believed [redacted] may have coordinated with DOJ, but not with the FBI.

In or around March and April 2015 [redacted] and IPS felt pressure by both Congress and internally from KENNEDY and [redacted] to quickly approve the 296 emails for release. Initially,

Continuation of FD-302 of [redacted] Interview of [redacted], On 08/17/2015, Page 3

[redacted] and his team were told to do a "light review with light redactions," but were later told by the Office of Legal Counsel to perform a regular FOIA review. [redacted] special team of senior reviewers, approximately 40 full-time equivalent reviewers, worked with the appropriate Bureaus on possible classified information and sent the proper referrals to the United States Intelligence Community (USIC) partners.

[redacted] did not think [redacted] and the Office of Legislative Affairs attorneys had the appropriate training and experience to review, redact and produce emails responsive to Congressional inquiries and especially not expert enough to respond to FOIA requests. For starters [redacted] and her team performed their entire review, redacted what they did, and then copied the 296 emails to a .pdf file on an unclassified network. If any information was later found to be classified, then they would have not only corrupted every computer that touched that classified information, but they might have contributed to a loss of classified data. IPS always pushed their material to the SIPRNET network and used their "F2" enclave to perform their FOIA review before disseminating their products. Also, the 296 emails provided by [redacted] via .pdf included redactions done for CLINTON's privacy but unrelated to national security.

[redacted] believed there was interference with the formal FOIA review process. Specifically, STATE's Near East Affairs Bureau upgraded several of CLINTON's emails to a classified level with a B(1) release exemption, [redacted] along with [redacted] attorney, Office of Legal Counsel called STATE's Near East Affairs Bureau and told them they could use a B(5) exemption on an upgraded email to protect it instead of the B(1) exemption. However, the use of the B(5) exemption, which is usually used for executive privilege-related information, was incorrect as the information actually was classified and related to national security, which would be a B(1) exemption.

In or around March or April 2015, there was a meeting where [redacted] told [redacted] [redacted] Information Services, [redacted] U.S. Department of Justice (DOJ), and [redacted] DOJ, that she had coordinated the review of the 296 emails with the appropriate STATE bureaus and inter-agencies. The emails "were already reviewed and there was nothing classified in them, so the FOIA review should go quickly." [redacted] was unsure why the FOIA review was taking so long.

[redacted] again stressed [redacted] review and coordination were done with people unfamiliar to [redacted] and were not the normal points of contact that IPS used for other agencies. More importantly, although [redacted] and [redacted] thought their quick initial review showed none of the 296 emails were sensitive, following the formal FOIA review, one document had been upgraded to classified based on input from [redacted] and [redacted]. There were other documents IPS recommended for upgrade, including one specifically related to the Department of Defense's United States Central Command (CENTCOM), and others that were still in the referral stage, including emails that have FBI and CIA equities involved that originated from BLUMENTHAL.

Continuation of FD-302 of [redacted] Interview of [redacted], On 08/17/2015, Page 4

[redacted] did not know why he and IPS were not part of the initial Congressional review for the 296 Benghazi-related emails, like they had been for past Congressional inquiries. [redacted] was cut out of the loop for the materials initially sent to Congress and had no idea what kind of review [redacted] and her team performed. [redacted] and [redacted] seemed to have been placed in their specific positions by top STATE officials; they appeared to have a very narrow focus on all CLINTON-related items, and were put in positions that were not advertised.

b6  
b7C

In early May 2015, KENNEDY called an interagency meeting regarding the scheduled release of all the CLINTON-related emails by the January 15, 2016 deadline and asked for quick turnarounds on any future requests. People in attendance included [redacted] representatives from White House Counsel, CIA, FBI, Office of the Secretary of Defense (OSD), Director of National Intelligence (DNI) and the National Security Council (NSC).

b6  
b7C

Immediately following that meeting, KENNEDY held a closed-door meeting with [redacted] and [redacted] DOJ's Office of Information Programs where KENNEDY pointedly asked [redacted] to change the FBI's classification determination regarding one of CLINTON's emails, which the FBI considered classified. The email was related to FBI counter-terrorism operations.

b6  
b7C

KENNEDY called [redacted] directly on one occasion. The purpose of that call was to ask [redacted] questions regarding pressure from the Office of the Inspector General of the Intelligence Community (ICIG) to complete the review of the approximately 30,000 emails. Specifically, KENNEDY wanted to know if there was precedent to have outside reviewers help STATE with the FOIA process. At that time [redacted] was unaware of STATE IG's and ICIG's June 19, 2015 joint recommendation to STATE regarding the FOIA review process. [redacted] ICIG, offered [redacted] and IPS extra reviewers from the intelligence community to help review the 30,000 emails. However, many of those reviewing officials arrived untrained to formally review items. After the initial training, those reviewers became instrumental to the review process.

b6  
b7C

[redacted] had not felt as much pressure regarding the review and release of the 30,000 emails as with the 296 Benghazi-related emails. [redacted]

b6  
b7C

[redacted] Instead of pressure, it felt more like curiosity as to the raw numbers of emails already reviewed, upgraded from unclassified to classified, referred to outside agencies, and/or released publicly. To date, approximately 1,600 referrals were made to USIC partners. Many of those emails discussed foreign governments and their leaders along with various sensitive telephone calls. Other emails existed that would later be referred to the USIC. Those emails included emails from STATE personnel discussing information lost as a result of the "Wikileaks" scandal.

Some material from the 30,000 emails, though unmarked as such, were definitely classified back in 2009-2012 and still remained classified. On the other hand, it was true some material (in general, not specific to the 30,000 emails) could have been previously classified, but were later downgraded. An



Continuation of FD-302 of Interview of [REDACTED], On 08/17/2015, Page 5

example would be CLINTON's travel schedule or security-related information based on specific times and places. It was a very large security concern for IPS when they heard some STATE employees assumed all documents on unclassified system were unclassified, based on being on an unclassified system and having no portion markings.

One email that was upgraded from the 30,000 emails was an email exchange between CLINTON and [REDACTED] former [REDACTED] where both individuals used their personal email addresses to discuss matters related to Russia. Despite this, [REDACTED] responded to KENNEDY's request for all STATE-related personal emails with a letter that stated [REDACTED] had no STATE-related emails in his personal email account.

STATE was normally able to complete classification upgrades very quickly. The upgrade would happen after STATE bureaus and other agencies determined, 1) how the information was obtained; (2) what the information was; (3) based on current global events/situations; or (4) because the information was, initially, improperly marked as unclassified.

[REDACTED] heard the argument that some of CLINTON's emails were unclassified back in the 2009-2012 timeframe when they were initiated, but were later classified due to various circumstances. It was very rare for something that was actually unclassified to become classified years after the fact. [REDACTED] National Archives would be a good point of contact for knowledge on the upgrading process in general.

On or about August 10, 2015, [REDACTED] from Office of the Secretary of Defense (OSD) called [REDACTED] and told her CENTCOM records showed approximately 1,000 work-related emails between CLINTON's personal email and General David PETRAEUS, former Commander of CENTCOM and former Director of the CIA. Most of those 1,000 emails were not believed to be included in the 30,000 emails that IPS was reviewing. Out of the 30,000 emails, IPS only had a few emails from or related to PETRAEUS, as well as a few related to Leon PANETTA, former Secretary of Defense. There were a lot of emails to/from Denis MCDONOUGH, former Deputy National Security Advisor and current White House Chief of Staff.

[REDACTED] described Jacob SULLIVAN and Cheryl MILLS as "gatekeepers" for sending CLINTON emails/material; they would filter or review most items that CLINTON would receive. [REDACTED] recommended the FBI talk to his boss, [REDACTED] specifically about individuals at STATE who hold a weekly meeting about Congressional records production and the FOIA process as well as where [REDACTED] felt pressure came from regarding upgrading any of the 296 Benghazi-related emails. [REDACTED] recommended the FBI should talk with [REDACTED] regarding the alleged 1,000 emails between CLINTON and PETRAEUS.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/27/2016

(U//~~FOUO~~) On June 23, 2016, MONICA HANLEY was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at [REDACTED] Washington, DC 20001. Representing HANLEY, and also present for the interview, were [REDACTED] and [REDACTED]. After being advised of the identities of the interviewing agents, and the purpose of the interview, HANLEY provided the following information:

b6  
b7C

(U//~~FOUO~~) HANLEY created an archive of HILLARY R. CLINTON's hdr22@clintonemail.com emails in March 2013 as a result of concerns related to a reported hack of SIDNEY BLUMENTHAL's email account. HANLEY recalled participating in a conference call with HUMA ABEDIN and JUSTIN COOPER following the hack to discuss changing CLINTON's email address. [REDACTED] may have also participated in the call. While the group ultimately decided together to change CLINTON's account, ABEDIN selected the new name of the email account, hrod17@clintonemail.com.

b6  
b7C

(U//~~FOUO~~) COOPER set up the email account and assisted HANLEY with the technical details concerning creating a backup of hdr22@clintonemail.com. COOPER provided HANLEY an Apple Mac laptop from the Clinton Foundation, which HANLEY took home to her apartment in [REDACTED]. HANLEY remotely signed on to CLINTON's email server from her apartment, as COOPER telephonically walked her through the steps to transfer the emails from the server to the laptop and a thumb drive. HANLEY used MacMail, a built in application on the laptop, to transfer the emails. HANLEY initiated the process, and left the computer running, as the entire transfer process took a few days.

b6  
b7C

(U//~~FOUO~~) CLINTON's email address was changed from hdr22@clintonemail.com to hrod17@clintonemail.com before the archive was created.

(U//~~FOUO~~) While HANLEY could not recall the specific model of the aforementioned Apple laptop provided by COOPER, she did recall the model was not an "Air," but was likely a "Pro" because it had an ethernet port and a thumb drive portal. HANLEY further provided that the laptop she received from COOPER was silver in color and seemed like a newer model. The thumb drive HANLEY used was something she happened to have laying around the house. She could not recall any details concerning the brand or appearance of the thumb drive.

Investigation on 6/23/2016 at Washington, D.C.

b3  
b7E

File # [REDACTED]-302 Date dictated N/A

By SA [REDACTED] SA [REDACTED]

b6  
b7C

Continuation of FD-302 of Interview of Monica Hanley, On 6/23/2016, Page 2

(U//~~FOUO~~) Although it never actually happened the way it was intended, the initial purpose for creating two backups of hdr22@clintonemail.com (one on the laptop and the other on the thumb drive) was so a backup was available at both CLINTON's New York and Washington, DC, residences. The laptop remained at HANLEY's apartment in [REDACTED] until she transitioned to a job in the [REDACTED] in early 2014. HANLEY thought the laptop was stored in a drawer or on the desk in her bedroom. HANLEY did not use the laptop after the transfer of emails, nor did she have knowledge of anybody else accessing the laptop. The laptop was also password protected, so it would be impossible for anybody to access the laptop without HANLEY's assistance.

b6  
b7c

(U//~~FOUO~~) HANLEY could not recall whatever came of the thumb drive she created, and searched her apartment multiple times in attempts to locate it. HANLEY thought she might have given the thumb drive to ABEDIN when she transitioned to [REDACTED] as she provided ABEDIN with several items upon departure. However, HANLEY did not specifically recall providing ABEDIN with said thumb drive.

b6  
b7c

(U//~~FOUO~~) After the emails were transferred from hdr22@clintonemail.com to the laptop and thumb drive, the intention was to delete the emails off the CLINTON email server. HANLEY would not have been involved with deleting emails, and assessed COOPER would have been responsible for deleting anything directly from the server.

(U//~~FOUO~~) In 2014, after she was no longer working for CLINTON, HANLEY realized she still had possession of the Macbook containing CLINTON's archived emails. HANLEY subsequently contacted Platte River Networks (PRN) on her own accord and spoke with [REDACTED]. HANLEY initially tried to remotely send [REDACTED] the archive via the following application, which [REDACTED] provided HANLEY via email:

b6  
b7c

<https://broker.gotoassist.com/h/citrixassist?Question=DR051-438-752>. HANLEY initially attempted to transfer the archive to [REDACTED] remotely from CLINTON's New York residence via the aforementioned website, however it did not work. HANLEY subsequently attempted to send the archive remotely from her own residence, and was also unsuccessful. HANLEY and [REDACTED] ultimately decided HANLEY would ship the laptop containing the archive to [REDACTED] and he would transfer the archive to CLINTON's PRN server. [REDACTED] was then going to wipe the laptop and return it to [REDACTED] who was CLINTON's [REDACTED] at the time. HANLEY shipped the laptop to [REDACTED] as they discussed, but was not aware of what happened to the laptop thereafter.

(U//~~FOUO~~) CLINTON did not know her email login information, as HANLEY would generally change the information in CLINTON's BlackBerry when necessary so CLINTON's email would automatically populate. When CLINTON's password required changing, HANLEY would choose a new password, update CLINTON's BlackBerry with the change, and notify ABEDIN, COOPER and BRYAN PAGLIANO. HANLEY had CLINTON's email logon information and password, so she could check CLINTON's email if needed. On occasion, CLINTON would ask HANLEY to research an old email that CLINTON was unable to pull up on her BlackBerry. In order to respond said request, HANLEY would

Continuation of FD-302 of Interview of Monica Hanley, On 6/23/2016, Page 3

open up CLINTON's email account remotely from a computer and print the document for CLINTON. HANLEY assumed ABEDIN also accessed CLINTON's email account on occasion.

(U//~~FOUO~~) HANLEY often purchased replacement BlackBerry devices for CLINTON when she was Secretary of State. CLINTON preferred BlackBerry devices that contained a roller-ball rather than the more modern touch pad. HANLEY recalled purchasing most of CLINTON's replacement BlackBerry devices from a Washington, DC, AT&T Store in DuPont Circle. HANLEY also recalled purchasing one BlackBerry from an AT&T store in the Pentagon City Mall in Arlington, VA. HANLEY also recalled purchasing a replacement BlackBerry for CLINTON from either Ebay or Amazon, but stated this took place after CLINTON's tenure at the Department of State.

(U//~~FOUO~~) HANLEY had little insight into the writing process of CLINTON's book/memoir. She recalled CLINTON meeting with the writers regularly for multi hour meetings, where she assumed CLINTON would share topics and anecdotes she wanted to cover in the book. HANLEY also printed out chapters of the memoir as it was being written so CLINTON could make edits. HANLEY had no knowledge of the writers having access to CLINTON's emails.

(U//~~FOUO~~) At the conclusion of the interview, HANLEY agreed to provide interviewing agents copies of emails she exchanged with [REDACTED]

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

FBI INFO.

CLASSIFIED BY: NSICG C28W34B64

REASON: 1.4 (C)

DECLASSIFY ON 12-31-2041

DATE 09-22-2016

Date of transcription 03/11/2016

(U//FOUO) On February 27, 2016, JACOB SULLIVAN, DOB [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED] at the FBI Washington Field Office, 601 4<sup>th</sup> Street NW, Washington DC. Present for the interview were SULLIVAN's attorneys Beth Wilkinson and Alexandra M. Walsh, from Wilkinson, Walsh & Eskovitz LLP. Also present was FBI Section Chief Peter P. Strzok, as well as David Laufman, [REDACTED] and [REDACTED] from the Department of Justice (DOJ). Prior to the interview, Wilkinson and Walsh agreed to sign a non-disclosure agreement in anticipation of viewing documents during the interview that were classified as part of a Special Access Program (SAP). After being advised of the identities of the interviewing agents, and the purpose of the interview, SULLIVAN provided the following information:

(U//FOUO) SULLIVAN was recruited by [REDACTED] to be an advisor for HILLARY CLINTON during her 2008 presidential campaign. When CLINTON became the Secretary of State in 2009, SULLIVAN became a Deputy Director of Policy Planning at the Department of State (DOS). In and around February 2011, [REDACTED] SULLIVAN became Chief of Staff and Director of Policy Planning at DOS. In this role, SULLIVAN managed and supervised approximately 30 people and his specific duties, and that of most senior officials at DOS, were prescribed by CLINTON. Under her tenure, SULLIVAN traveled with CLINTON on almost every business trip she took and acted as a conduit to the National Security Council (NSC). SULLIVAN produced policy papers and proposals with a goal of staying ahead on regional issues and thinking "beyond day-to-day." SULLIVAN recalled coordinating his official written products to CLINTON through a "clearance process" filtered through career Foreign Service Officers (FSO) and executive assistants [REDACTED] and [REDACTED]. SULLIVAN would also email CLINTON directly related to a variety of topics. These communications included emails written by SULLIVAN, as well as emails SULLIVAN would forward to CLINTON based on his judgement as to their relevance. SULLIVAN also participated in Principal's Committee (PC) meetings with CLINTON in the Situation Room.

(U//FOUO) Every morning throughout her tenure as Secretary of State, CLINTON would head an 8:45am meeting with her deputies to discuss a broad range of topics related to policy formulation. These deputies included SULLIVAN, [REDACTED], [REDACTED] WILLIAM BURNS, and CLINTON's legal advisor and Chief of Staff CHERYL MILLS. SULLIVAN described MILLS as a

Investigation on 02/27/2016 at Washington DC

File # [REDACTED] Date dictated N/A

by SA [REDACTED] SA [REDACTED]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~

b1  
b3

b6  
b7C

b6  
b7C

b6  
b7C

b3  
b7E

b6  
b7C

b1  
b3

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of Interview of Jake Sullivan, On 02/27/2016, Page 2

traditional Chief of Staff and a "hands-on manager" who "empowered" people. SULLIVAN believed MILLS was involved in all "consequential" decisions made by CLINTON. SULLIVAN described HUMA ABEDIN as CLINTON's Deputy Chief of Staff for Operations. In this role, ABEDIN handled day-to-day operations to include scheduling and trip planning for CLINTON. SULLIVAN described ABEDIN as a close confidant of CLINTON and as someone who had a "trusted relationship" with CLINTON.

(U//~~FOUO~~) SULLIVAN had two computer systems in his office on the 7<sup>th</sup> floor at DOS Headquarters (HQ): one on the Secure Internet Protocol Router Network (SIPRnet), authorized to handle classified information up to the Secret level and one on an unclassified network. SULLIVAN had an official DOS email account on both of the foregoing networks. Due to size restrictions on SULLIVAN's email accounts, he often had to "archive" emails to create space in his email account. SULLIVAN recalled archiving email in "big chunks" but otherwise, could not recall any methodology or science he applied when archiving email. It was SULLIVAN's practice to use his state.gov email account for all DOS related business. SULLIVAN did recall occasionally using his personal google email (gmail) account for DOS business when traveling and on the weekends. Although SULLIVAN could log-in to his state.gov email account while away from the office, he used his gmail account for DOS business because it was sometimes difficult to log-in to his state.gov email account from his residence on the weekends and while traveling. SULLIVAN could not recall any DOS guidance involving the use of personal email for work purposes. SULLIVAN could not recall any guidance from CLINTON regarding the use of personal email for work purposes. At some point in his DOS career, SULLIVAN recalled receiving some form of notification that Chinese actors were targeting the gmail accounts of DOS employees. SULLIVAN did not recall taking any action as it related to this notification. SULLIVAN, MILLS, and ABEDIN did not have access to the Joint Worldwide Intelligence Communication System (JWICS) at the DOS. SULLIVAN recalled being briefed on the elements of information security upon indoctrination to the DOS. SULLIVAN understood the DOS "upclass" process as an unclassified document that at some point, or when combined with other documents, would become classified. SULLIVAN could not provide an example to this effect.

(U//~~FOUO~~) SULLIVAN had secure telephone equipment in his office on the seventh floor at the DOS. SULLIVAN was issued a BlackBerry mobile device by the DOS and did not recall receiving an upgraded handset during his tenure. SULLIVAN could not recall being issued a secure mobile phone by the DOS. SULLIVAN recalled being issued a secure mobile phone by the White House for a weekend, but could not recall anything further about this device or his use of it.

(S//~~NF~~) When traveling overseas for his work at the DOS, SULLIVAN recalled being briefed on information security pertaining to the threat in certain countries. For instance, SULLIVAN recalled an unclassified briefing at Joint Base Andrews where the Diplomatic Security Service (DSS) warned of a heightened level of physical and electronic surveillance in Russia. Because of this threat, SULLIVAN recalled [REDACTED] SULLIVAN also

b1 per DOS

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~b1  
b3Continuation of FD-302 of Interview of Jake Sullivan, On 02/27/2016, Page 3

recalled [REDACTED] Since SULLIVAN traveled with secure DOS communication systems while traveling overseas, SULLIVAN would make a secure call, conduct a secure video teleconference, or use the secure computers provided on the plane if a conversation needed to take place at the classified level. SULLIVAN recalled the [REDACTED] SULLIVAN had no memory of abnormal security screening or unusual functionality of his electronic devices while traveling overseas. SULLIVAN did not conduct foreign travel for personal reasons while at the DOS.

b1 per DOS

b1  
b3

(U//~~FOUO~~) SULLIVAN recalled CLINTON had a Secure Compartmented Information Facility (SCIF) in her residence in Washington DC with secure phone and fax equipment. CLINTON also received information at her DC residence via courier. SULLIVAN could not recall if CLINTON had a SIPRnet computer terminal in her residence. SULLIVAN would primarily transmit or communicate classified information to CLINTON at her DC residence through a secure call. SULLIVAN could not recall if CLINTON used a secure mobile phone. SULLIVAN was not familiar with the infrastructure in CLINTON's home in Chappaqua, but assumed it had the same capabilities as her DC residence. SULLIVAN did not know if CLINTON had staff at her residences that also held security clearances.

(U//~~FOUO~~) SULLIVAN recalled CLINTON had an "enormous" amount of information, to include classified information, briefed to her in-person or provided to her through paper flow. CLINTON would routinely digest the Presidential Daily Brief (PDB) in paper form and conduct policy meetings daily. SULLIVAN recalled little to no classified information passed to CLINTON electronically. In most instances, if information needed to be sent to CLINTON, it was routine that a senior FSO in the DOS Operation Center on the 7<sup>th</sup> floor of DOS HQ would facilitate the transmission. If CLINTON needed to be present to receive the information, as in the case of a secure call or fax, coordination would be done through CLINTON's assistants.

(U//~~FOUO~~) SULLIVAN recalled CLINTON used a personal email address when she worked in the Senate and while she was at the DOS, but was unaware email was hosted on a private email server in her residence until it became public knowledge in March 2015. Moreover, SULLIVAN knew JUSTIN COOPER and BRYAN PAGLIANO, but never had a conversation with them regarding any private email server. SULLIVAN had no memory of a conversation regarding federal records retention or FOIA implications as it related to the use of private email. SULLIVAN knew the general guidelines at the DOS related to federal records retention. For example, SULLIVAN knew not to delete email from his DOS email accounts. Upon leaving DOS, SULLIVAN boxed up his official DOS paper records and turned them over to the DOS. SULLIVAN recalled the DOS handled the preservation of his email records from DOS servers. SULLIVAN recalled one brief conversation in the summer of 2014 with MILLS and [REDACTED] pertaining to the production of federal records, but could not recall more detail.

b6  
b7C

(U//~~FOUO~~) The email address SULLIVAN recalled CLINTON using was hdc22@clintonemail.com. SULLIVAN also recalled that HUMA ABEDIN had a @clintonemail address.

~~TOP SECRET~~b1  
b3

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

Continuation of FD-302 of Interview of Jake Sullivan On 02/27/2016, Page 4

but could not remember it specifically. SULLIVAN was never asked to have a @clintonemail address and never requested that one be issued to him. SULLIVAN was unaware of any back-ups, migration, deletion or wiping of email from the clintonemail.com domain. SULLIVAN recalled a conversation with HEATHER SAMUELSON in the fall of 2014 where SAMUELSON told SULLIVAN he may need to look through documents to see if they constitute a federal record, but this process never occurred.

(U//~~FOUO~~) Upon initiation of his employment at DOS, SULLIVAN received a TOP SECRET (TS) Sensitive Compartmented Information (SCI) security clearance. In order to receive the foregoing clearance, SULLIVAN recalled an orientation and briefing where handling, transporting, and disseminating classified information was discussed. As far as he understood, SULLIVAN had derivative classification authority and could classify information based on the guidance of a classification manual. Other than CLINTON, SULLIVAN was unaware of anyone at DOS that had Original Classification Authority (OCA). As part of his job, SULLIVAN was briefed into a large number of SAP and covert action programs. The process of being briefed into a SAP required an individual from the DOS Bureau of Intelligence and Research (INR) to brief the program and ensure the requisite forms were signed and maintained. SULLIVAN did not recall ever handling SAP material on a TS computer system, but was aware INR had TS computer systems.

b1  
b3

[REDACTED]

(U//~~FOUO~~) SULLIVAN stated a PC meeting would be initiated by the NSC chair and would require the staff of the government agencies invited to prepare a package regarding whatever topic the NSC would prescribe. As a Standard Operating Procedure (SOP), a PC would initiate a Deputy's Committee (DC) meeting where certain subject matter experts in each agency would deliberate on their agency's conclusion pertaining to the prescribed topic. For the DOS, the bureaus that covered the topic of the PC meeting would author packages and then funnel them through [REDACTED] and [REDACTED] to CLINTON for use in the PC meeting. SULLIVAN would sometimes be involved in DC meetings if his bureau had a stake in the issue. In that instance, SULLIVAN would author sections of written packages that covered the issue. SULLIVAN would gain his knowledge and source his document through a combination of things he read, conversations he had and classified information. When the PC occurred, each agency would usually bring their Principal plus one other representative. For the DOS, it was often CLINTON and the respective Deputy that attended a PC meeting. SULLIVAN attended PC meetings "occasionally" and could not recall a precise amount.

b6  
b7C

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1  
b3



~~TOP SECRET~~ [redacted] ~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

(Continuation of FD-302 of [redacted] interview of Jake Sullivan, On 02/27/2016, Page 5)

(U//FOUO) After reviewing an email dated June 17, 2011 with subject line "Plan for PC tomorrow," SULLIVAN stated he did not remember the email specifically. SULLIVAN stated he had already viewed this email when released by the DOS through a Freedom of Information Act (FOIA) request. SULLIVAN did not recall the specific email or what the PC meeting was about. SULLIVAN understood "nonpaper" to mean an unclassified document without official markings given to a foreign government that states the unofficial position of the US government. SULLIVAN understood "nonpaper" to mean this because he had created a "nonpaper" document for CLINTON before. In the context of the displayed email, and while reading it in the moment, SULLIVAN thought CLINTON would have wanted him to make an unclassified version of the document, summarize the contents, and then send it to her on a nonsecure fax. SULLIVAN stated that CLINTON took the protection of classified information very seriously.

(S//NF) After reviewing an email dated October 13, 2012, with subject line "Fw: This am Green on Blue," SULLIVAN stated he did not remember the email specifically. [redacted]

b1  
b3  
b7E

[redacted] SULLIVAN knows [redacted] and first met him while [redacted] SULLIVAN worked as colleagues with [redacted] when [redacted] was at the Pentagon and CIA.

(U//FOUO) After reviewing an email dated April 10, 2011, with subject line "Fw: Stevens Update (Important)," SULLIVAN stated he did not remember the email specifically. SULLIVAN did not think the email was unusual and wasn't surprised AFRICOM information would be cited in an unclassified email. SULLIVAN would regularly review situation reports from around the world in unclassified email. SULLIVAN knew [redacted] as a career FSO that worked in the DOS Operation Center. SULLIVAN stated [redacted] would regularly share events from around the world in unclassified email and had no reason to question [redacted] judgement regarding the proper handling of classified information.

b6  
b7C

[redacted] After reviewing an email dated December 27, 2011, with subject line "FW: (SBU)," SULLIVAN stated he did not remember the email specifically. [redacted]

b1  
b3

[redacted] SULLIVAN had no reason to believe any DOS employees he worked with ever intentionally mishandled classified information and did the best they could to make a sound judgement when handling classified information. [redacted]

~~TOP SECRET~~ [redacted] ~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~

~~NY~~

FD-302a (Rev. 10-6-95)

b1  
b3

Continuation of FD-302 of Interview of Jake Sullivan On 02/27/2016 Page 6

(U//~~FOUO~~) After reviewing an email dated July 4, 2009, with subject line "Fw: Follow Up: Summary of 1055 EDT DPRK Conference Call," SULLIVAN stated he did not remember the email specifically. SULLIVAN did not specifically recall the name [REDACTED] SULLIVAN did recall the name [REDACTED] and knew her to be a senior Watch Officer in the DOS Operation Center. When asked about the content of the email and if he believed the pending military activities of a foreign military was classified, SULLIVAN replied the person at DOS who sent the email must have had reason to believe it could be sent on an unclassified system. SULLIVAN stated everyone he worked with at DOS worked hard while under pressure and used the best judgement they could to accomplish the mission. SULLIVAN was unsure why [REDACTED] forwarded this particular email to his gmail account, but recalled being in Idaho around this time for a bachelor party. SULLIVAN stated that procedure was not routine practice for [REDACTED] and could not recall another instance where it occurred.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated April 27, 2012, with subject line "Fw: Day 2," SULLIVAN stated he did not remember the email specifically. SULLIVAN knew the "IA process" to mean Interagency process. SULLIVAN recalled the general subject matter of the email and remembers [REDACTED] trying to open the Ground Lines Of Communication (GLOC) between countries after attacks involving the International Security Assistance Force (ISAF).

b6  
b7C

(S//~~FOUO~~) After reviewing an email dated August 25, 2010, with subject line "Fw: NY Times article on Salehi," SULLIVAN stated he did not remember the email specifically. SULLIVAN did not recall the name SALEHI [REDACTED]

b1  
b3

[REDACTED] At the time, [REDACTED] was the [REDACTED] [REDACTED] and had the ability to email CLINTON directly, as well as forward email to SULLIVAN.

[REDACTED] After reviewing an email dated July 6, 2012, with subject line "Fw: US drone strike kills 4 militants in Pakistan," SULLIVAN stated he did not remember the email specifically. [REDACTED]

b1  
b3

[REDACTED] After reviewing an email dated February 25, 2012, with subject line "Fw: Alert," SULLIVAN stated he did not remember the email specifically, but recalled seeing this redacted email in a FOIA release by the DOS. [REDACTED]

b1  
b3

~~TOP SECRET~~

~~NY~~

b1  
b3

~~TOP SECRET~~

~~NT~~

b1  
b3

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of Interview of Jake Sullivan, On 02/27/2016, Page 7

[redacted] After reviewing an email dated [redacted] with subject line [redacted] SULLIVAN stated he did not remember the email specifically. SULLIVAN stated that, based on the subject line, [redacted] was reporting in a manner he believed to be sensitive but unclassified. SULLIVAN stated [redacted] may have sent this email on an unclassified system because the drone strike could have already hit the news wire. SULLIVAN did not believe reporting on a drone strike after the fact made it less sensitive, but was speculating on [redacted] inducement. SULLIVAN believed [redacted] reference to a "secure call" in the email demonstrated [redacted] attempt to delineate between what could go in unclassified and classified channels. Additionally, SULLIVAN stated this email was not out of step with how people approached similar matters at the time. Nothing stood out to SULLIVAN at the time as mishandling classified information.

b1  
b3

(U//FOUO) After reviewing an email dated May 16, 2011, with subject line "Re: Senator Kerry has requested to speak with Secretary Clinton," SULLIVAN stated he had a general recollection of the event discussed in the email, but did not recall the email specifically. SULLIVAN did not recall the conversation with [redacted] referenced in the email.

b6  
b7C

(S) ~~(U//FOUO)~~ After reviewing an email dated August 24, 2011, with subject line "Re: Rasmussen call," SULLIVAN stated he did not remember the email specifically. SULLIVAN stated he usually found out about [redacted] through open source reports, DOS email reflecting news accounts and more rarely, through someone in the DOS HQ building.

b1

[redacted] After reviewing an email dated [redacted] with subject line [redacted] SULLIVAN stated he did not remember the email specifically. SULLIVAN stated the email was "unusual" and he could not determine what he was referring to by the [redacted] but he was not sure.

b1  
b3

[redacted] After reviewing an email dated [redacted] with subject line [redacted] SULLIVAN stated he did not remember the email specifically. SULLIVAN stated the call with [redacted] regarding the nomination of a second strike was with [redacted] SULLIVAN stated he infrequently communicated with [redacted] and, when he did, it was through a mix of secure calls, unclassified calls and unclassified emails.

b1  
b3

[redacted] After reviewing an email dated [redacted] with subject line [redacted] SULLIVAN stated he did not remember the email specifically. SULLIVAN did not recall how he communicated with [redacted] and guessed it was not by phone and most likely, SULLIVAN cut and pasted from another unclassified email. SULLIVAN did not recall speaking with [redacted] generally. While working at the DOS, SULLIVAN stated he can't recall one time he felt uneasy about something he read in an unclassified email. SULLIVAN could not recall an instance where anyone expressed a concern with the type of information coming over the unclassified email system or

b1  
b3

~~TOP SECRET~~

~~NT~~

b1  
b3

~~TOP SECRET~~



~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of Interview of Jake Sullivan On 02/27/2016, Page 8

with handling classified information in general. SULLIVAN stated CLINTON never expressed a concern about the handling of classified information. While at the DOS, SULLIVAN felt his colleagues judgement was good and that they had a good understanding of how to handle classified information. Generally, while at the DOS, SULLIVAN stated he had to pay attention to what information goes on what channel. For instance, he would convey what he could on an unclassified system and then go to equipment authorized to handle classified communications to convey more information.

(U//~~FOUO~~) After reviewing an email dated October 4, 2009, with subject line "FW: Cover memo," SULLIVAN's attorney, BETH WILKINSON, asked for the classification of the email. After being advised the email was pending classification review and to treat the email as classified, WILKINSON stated her client would not answer questions related to the foregoing email, or any documents related to the email.

(U//~~FOUO~~) SULLIVAN stated SYDNEY BLUMENTHAL was someone CLINTON knew from years back and was someone who "liked to help the cause." As SULLIVAN understood it, BLUMENTHAL had a variety of sources of information. SULLIVAN was unaware of the identities of the sources used by BLUMENTHAL. SULLIVAN recalled BLUMENTHAL would sometimes refer to information he gathered from former intelligence officers, but SULLIVAN understood those people to be retired with no access to classified information. SULLIVAN would occasionally talk to BLUMENTHAL through phone conversations and maybe through email. In those conversations, BLUMENTHAL would relay information about "big picture" topics BLUMENTHAL thought were relevant and SULLIVAN would pass it on to CLINTON or DOS stakeholders to have them validate the information. SULLIVAN never heard of a concern that BLUMENTHAL had access to, or was relaying, classified information.

(U//~~FOUO~~) The original notes of the interview, signed aforementioned non-disclosure agreements, and documents displayed to SULLIVAN will be maintained in a FD-340 envelope and filed with the captioned investigation.

~~TOP SECRET~~



~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/21/2015

(U//~~FOUO~~) PATRICK FRANCIS KENNEDY, Under Secretary of State for Management, was interviewed at his office at Department of State (DoS), Harry S. Truman Building, 2201 C Street NW, Washington, D.C., by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED]. Also present for the interview was FBI National Security Law Branch (NSLB) Attorney [REDACTED] and Senior DoS Counsel [REDACTED]. After being advised of the identity of the interviewing agents, and the nature of the interview, KENNEDY provided the following information:

b6  
b7C

(U//~~FOUO~~) KENNEDY was aware Secretary of State HILLARY CLINTON used a personal email account during her tenure as Secretary, but was unaware that she was using a personal server. KENNEDY received an unclassified email from CLINTON approximately once a month and noted those emails came from a clintonemail.com address.

(U//~~FOUO~~) The DoS "GO" system allows for DoS employees to remotely access their DoS account from a non-DoS server. DoS policy does not support the routine use of private email accounts for DoS business. However it was understood that exceptions could be made in emergency situations, and in doing so, the employee should carbon copy their DoS email account for matters of record.

(U//~~FOUO~~) KENNEDY mostly received emails from CLINTON after hours, and so infrequently he was not aware of the volume of which she was using her personal account. KENNEDY was not aware CLINTON was solely using a personal email account for communicating unclassified DoS business.

(U//~~FOUO~~) DoS policy does not support the use of private email servers for continued personal use, nor the use of personal servers for DoS business, thus there is no approval process for their use. DoS policy remains the same for the use of both personal emails and servers today as it was during CLINTON's tenure.

(U//~~FOUO~~) KENNEDY recalled news stories implying a former DoS employee, BRYAN PAGLIANO, set up CLINTON's private email and server "on the side" while working for DoS. However, KENNEDY noted he was not aware of PAGLIANO's involvement until it hit the press. DoS is refraining from direct inquiries into PAGLIANO's involvement until the FBI completes its investigation.

Investigation on 12/21/2015 at Washington, D.C.

File # [REDACTED] 302 Date dictated N/A

b3  
b7E

By SA [REDACTED] SA [REDACTED]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of Interview of Patrick F. Kennedy, On 12/21/2015, Page 2

(U//~~FOUO~~) KENNEDY had no direct knowledge of any of CLINTON's predecessors [COLIN POWELL and CONDOLEEZZA RICE] using private email accounts, but noted he was aware POWELL publically mentioned he used a private email account during his tenure as Secretary of State in his most recent publication.

(U//~~FOUO~~) DoS has the responsibility of interfacing with foreign diplomats and political representatives within the United States and overseas to help develop policy. Sometimes information from these dignitaries is given in confidence and sometimes it is not. The classification of such information is specific to the situation. KENNEDY explained that information given in confidence may be initially transmitted as unclassified to report the information, but later "up-classified" when it is further assessed the disclosure of such information might damage national security or diplomatic relationships. Ultimately, the originator of a document or email is responsible for classifying the document.

(U//~~FOUO~~) KENNEDY explained the Intelligence Community (IC) "steals" information, and thus has to classify said information to protect sources and methods. DoS may get the same information through diplomatic channels and not classify that information because it was not received from a sensitive source or a method. According to KENNEDY, the classification of a DoS document depends on the content of the message and if it is important for the other party not to disclose the information.

(U//~~FOUO~~) If a DoS employee wanted to use classified information derived from IC sources in an unclassified channel, they would need to submit a tearline request to do so. DoS cannot declassify a document that was not originally classified by a DoS classification authority.

(U//~~FOUO~~) The Secretary of State is a declassification authority, as are the Secretary's Chief of Staff and Deputy Chief of Staff. KENNEDY believed CHERYL MILLS, JAKE SULLIVAN, and possibly HUMA ABEDIN would have been classification authorities during CLINTON's tenure at DoS.

(U//~~FOUO~~) KENNEDY acknowledged DoS received their first request to produce emails related to CLINTON's email sometime in 2014. The request was related to a Congressional inquiry concerning documents related to the 2012 attack of the United States consulate in Benghazi. The initial request was focused on specific emails, but was later expanded to include a broader production.

(U//~~FOUO~~) KENNEDY was not part of the initial dialogue with CLINTON concerning the aforementioned request for emails. KENNEDY was only involved with interacting with Congress concerning the status of the request, but was not involved in the process of deciding what was and was not released in response. The DoS Freedom of Information Act (FOIA) team directly handled the request by reaching out to the appropriate Bureau or Secretariat who maintained the information concerning Benghazi. The Bureau of Near East Affairs would have been contacted by FOIA in regards to general Benghazi information. [REDACTED] The DoS

b6  
b7c

Continuation of FD-302 of Interview of Patrick F. Kennedy, On 12/21/2015, Page 3

FOIA team would have reached out to the records staff in the Executive Secretariat for specific CLINTON communications concerning Benghazi.

(U//~~FOUO~~) DoS FOIA inquiries are handled by the Bureau of Administration/ Global Information Services, [REDACTED] The DoS Bureau involves a team of supervisors, processors and reviewers, almost all of which are retired foreign or civil service. The supervisors assign the requests to processors who load the information into their FOIA management system and send out requests to all the Bureaus who have a relevant relation to the request. The review team collects the information received from the relevant Bureaus and determines what if any exemptions should be considered and/or applied. The FOIA review team also determines if the information responsive to the request contains any outside agency equities, and appropriately coordinates with those agencies to respond to the request. Furthermore, the FOIA response goes through a review and reconciliation process to ensure all responsive documents are marked and redacted appropriately. [REDACTED] in regards to the DoS FOIA process. However, there is an appeals process which involves a FOIA review board managed out of the DoS Information Oversight Office. b6 b7c

(U//~~FOUO~~) Responsive documents to FOIA requests are also placed on the DoS FOIA website in their releasable form to avoid redundant FOIA requests from other parties.

(U//~~FOUO~~) KENNEDY recalled discussions concerning CLINTON wanting to cull her emails prior to producing emails related to the Congressional/FOIA requests. The purpose of the cull was to remove emails related to personal communications between CLINTON and her family that were not relevant to DoS matters. DoS was not involved in the cull, as it is the responsibility of the individual to produce records of relevance for the record. KENNEDY did not recall who was involved in assisting CLINTON cull her emails.

(U//~~FOUO~~) DoS employees identify their own files for the record and can generally archive them in the State Messaging and Archival Retrieval Toolset (SMART) system, which allows for electronic marking/tagging of emails for the record. However, SMART is not used by the Executive Secretariat, thus CLINTON would have likely had to use a print and file system, or simply keep all of her emails for the record. As a matter of personal preference, KENNEDY retains all of his electronic DoS communications in an active file.

(U//~~FOUO~~) When asked in retrospect if he had concerns over how DoS conducted its response to the FOIA request regarding CLINTON's emails, KENNEDY responded "yes and no." KENNEDY did not elaborate. KENNEDY further explained he contacted the FBI Deputy Director and requested an electronic copy of all the CLINTON emails turned over to the FBI in regards to the FBI's investigation, so DoS could make a better assessment in regards to evaluating their role/response.

Continuation of FD-302 of Interview of Patrick F. Kennedy. On 12/21/2015. Page 4

(U//~~FOUO~~) KENNEDY "categorically rejected" allegations he attempted influence FOIA markings to protect and/or mask classified information. KENNEDY [REDACTED] and described her as someone who "says it like it is" and has "no fear of telling truth to power." KENNEDY further explained he has full confidence [REDACTED] would not allow undue influence to effect her ability to properly carry out the FOIA process in accordance with the Presidents mandate to both air on the side of transparency and national security.

b6  
b7C

(U//~~FOUO~~) KENNEDY was one of three people he was aware of at DoS who have the authority to upgrade the classification of a document, the Secretary of State and [REDACTED] being the other two. A classification upgrade would be warranted in a situation where the change in a government may change relationships, and information that would not have endangered the United States or sources before said government change would then be considered a threat to national security or to the sources safety.

b6  
b7C

(U//~~FOUO~~) KENNEDY stated he was available for re-contact should interviewing agents have additional questions to ask at a later date.

(U//~~FOUO~~) Agent notes are maintained in a 1A envelope.



~~SECRET~~

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/18/2015

(U//~~FOUO~~) On December 14, 2015, [redacted]  
[redacted] Information Resource Management/Executive Secretariat, US Department of State, office phone  
[redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted]  
[redacted] and SA [redacted]. After being advised of the identity of the interviewing agents  
and the nature of the interview, [redacted] provided the following:

b6  
b7C

(U//~~FOUO~~) [redacted] in Information Resource Management  
(IRM) for the Executive Secretariat (IRM/ES) and was in that position during Secretary HILLARY  
CLINTON's time in office. Part of [redacted] job was to maintain and support the infrastructure for  
the UNCLASSIFIED and SECRET networks for the Executive Secretariat. Every Department of State,  
hereafter State, Secretary [redacted] has interacted with, except for Secretary JOHN KERRY, has used  
personal email during his or her time in office. For example, Secretary COLIN POWELL used America  
Online. Secretary Clinton, however, was the first Secretary to use a privately maintained email server,  
hereafter Server. [redacted] did not agree with the decision, but it made sense to him because  
Secretary CLINTON had used the Server for the previous two years. Secretary CLINTON did not have a  
desktop computer in her office to access email while at State, but did have non-SCIF space near her office  
where she could use her BlackBerry. [redacted] believed Secretary CLINTON received an  
operational security briefing that involved the National Security Agency after being sworn in as Secretary  
of State. [redacted] from the Bureau Security Office would have coordinated the briefing.

b6  
b7C

(U//~~FOUO~~) [redacted] became aware of Secretary CLINTON's Server at the time she was  
sworn in as Secretary of State. She was offered a State email address, but decided to use the Server from  
her 2008 presidential campaign. It was at this time [redacted] met BRYAN PAGLIANO.  
PAGLIANO was the administrator for Secretary CLINTON's Server, so [redacted] interacted with  
him to keep it communicating with State systems. For example, there were approximately 5-6 instances  
where emails sent by Secretary CLINTON to State employees, or vice-versa, were not received by the end  
user. In these instances, [redacted] and PAGLIANO worked together to modify settings so the emails  
would make it through. Additionally, the two worked to establish transport layer security (TLS) between  
State systems and the Server as a security measure.

b6  
b7C

(U//~~FOUO~~) Since PAGLIANO was an IRM Schedule C employee of State, [redacted] invited  
him to various briefings regarding security and system vulnerabilities. PAGLIANO's job at State was  
policy development related to mobile computing, so these briefings were also relevant to his role in that  
capacity. [redacted] specifically recalled discussions about Bluetooth vulnerabilities and blue jacking,  
because

b6  
b7C

Investigation on 12/14/2015 at Washington, DC

File # [redacted] 302 Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it  
and its contents are not to be distributed outside your agency.

~~SECRET~~

Continuation of FD-302 of Interview of [REDACTED], On 12/14/2015, Page 2b6  
b7C

those vulnerabilities were [REDACTED] primary concern due to Secretary CLINTON's BlackBerry use. Although [REDACTED] made an effort to keep PAGLIANO informed of security matters, he was not involved in decisions regarding Server security, nor does [REDACTED] know if the Server was hacked or actively monitored for intrusions. [REDACTED] did not believe it was possible for PAGLIANO to secure the Server as well as State servers, which are monitored and hardened by a team of full time employees. Additionally, he did not know how the Server was paid for or where it was physically located.

b6  
b7C

(U//~~FOUO~~) In approximately February 2011, several State employees were the victims of a gmail and yahoo hack where users received an email with a link directing them to change their email password. The link took users to a fraudulent site that allowed [REDACTED] to obtain the user's gmail/yahoo password. The hackers then used the password to modify the users gmail/yahoo account to auto-forward to a [REDACTED] [REDACTED] group sent a security alert to POEMS users regarding the b1 per DOS hack, but since PAGLIANO was not a POEMS user, he would not have received the alert.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was asked to delete approximately two emails related to the public release of Secretary CLINTON's emails. The request was in relation to cleaning unclassified State systems, however, due to an FBI preservation request, [REDACTED] had not deleted any communications. He recalled one of the emails being from an Ambassador and began with a phrase similar to "My classnet is down, so I'll start here..." [REDACTED] could not recall any other details, but offered to provide a copy of the emails if requested. There were no spills of classified information on Secretary CLINTON's email account while she was at State insofar as [REDACTED] was aware.

b6  
b7C

(U//~~FOUO~~) Secretary CLINTON received classified information in a paper briefing book that was maintained by her special assistant. When outside of Washington, DC, State travel teams turned hotel rooms into classified information processing areas where personnel, including the Secretary, could communicate securely.

(U//~~FOUO~~) Only Secretary CLINTON's inner circle could email her directly. This group consisted of JAKE SULLIVAN, CHERYL MILLS, and HUMA ABEDIN for State Department purposes. For this reason, when [REDACTED] emailed ABEDIN's BlackBerry, he considered it the equivalent of emailing Secretary CLINTON.

b6  
b7C

(U//~~FOUO~~) [REDACTED] stated the FBI's investigation would be incomplete without talking to PAGLIANO. PAGLIANO is a very sharp and technically savvy individual who likely took action based on the security information and briefings provided by [REDACTED] and others. Furthermore, [REDACTED] believes additional information could exist on the accounts of MILLS because she served as a proxy for Secretary CLINTON.

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/05/2015

STEVE A. LINICK, Inspector General, United States Department of State, Office of Inspector General (STATE IG), 2121 Virginia Avenue, NW, Suite 8100, SA-3, Washington, DC 20037, telephone [REDACTED] mobile phone [REDACTED] email [REDACTED]@state.gov was interviewed in person by FBI Special Agents [REDACTED] and [REDACTED]. After being advised of the identity of the interviewing Agents and the nature of the interview, LINICK provided the following information:

b6  
b7c

On or about March 12, 2015, STATE IG received a letter from U.S. Senators Bob Corker, Richard Burr and Ron Johnson. The letter requested a review of State Department employees' usage of personal email for official purposes and coordination with relevant agencies to determine whether classified information was transmitted or received by State Department employees over personal systems. On April 16, 2015, pursuant to this letter, STATE IG initiated a review of the use of personal communications hardware and software by five Secretaries of State and their immediate staffs. The review covered current Secretary of State John Kerry all the way back to former Secretary of State Madeleine Albright. STATE IG's review was further broken down into three categories 1) On-boarding Process (which looked into the approval process for the use of personal networks); 2) Preservation of Records (how records were maintained/preserved); and 3) the FOIA response.

LINICK believed STATE IG's office was not qualified to determine whether classified information was transmitted and referred that portion of the review to the Office of the Inspector General of the Intelligence Community (ICIG). Separately, STATE IG had the Benghazi review and [REDACTED]. The Department of State was also conducting a Freedom of Information Act (FOIA) review of fifty five thousand pages of emails belonging to Secretary Clinton pursuant to a court order. In December 2014, the Department of State received hard copies of those documents from Secretary Clinton's Counsel.

b6  
b7c

LINICK initially believed Department of State received electronic copies of Secretary Clinton's email from her private server. During a July 1, 2015 meeting with STATE IG, Patrick KENNEDY, Under Secretary for Management, U.S. Department of State and [REDACTED] advised STATE IG the Department of State had obtained an electronic copy of Secretary Clinton's email. On July 10, 2015, STATE IG requested two copies of the .PST files for use by STATE IG and ICIG. Later, KENNEDY advised STATE IG that the Department of State only had hard copies of the documents, which were

b6  
b7cInvestigation on 08/04/2015 at Washington, DCFile # [REDACTED] Date dictated N/Ab3  
b7EBy SA [REDACTED] SA [REDACTED]b6  
b7c

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of Interview of Steve A. Linick, On 08/05/2015, Page 2  
 scanned and uploaded to ClassNet. LINICK obtained preserved Department of State email records for MILLS and ABEDIN.

On May 26, 2015 ICIG and STATE IG sent a joint preservation letter to Williams & Connolly for the @clinontone.com account records in their possession. Although, LINICK was generally aware of the status of ICIG's ongoing review to identify classified information, which consisted of jointly working with the Department of State FOIA staff, LINICK was not heavily involved in that process. LINICK recommended the FBI interview Department of State employees [redacted] Office of Information Programs and Services and [redacted] Office of Global Information Services. Both [redacted] and [redacted] were involved in the FOIA review process and alleged there were potentially hundreds of classified emails found during their review. [redacted] further alleged that two [redacted] [redacted] currently working at State Department were meddling with the FOIA review process.

b6  
b7C

On or about June 19, 2015 STATE IG and ICIG jointly made four recommendations to the State Department related to the FOIA review process. The recommendations were as follows:

1. Recommend State Department FOIA office request staff support from IC FOIA offices to assist in the identification of intelligence community equities;
2. Recommend IC FOIA officers review the emails to ensure that ClassNet use is appropriate before transmitting to the State Bureaus for review;
3. Recommend State Department FOIA seek classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified materials; and
4. Recommend State Department FOIA Office incorporate the Department of Justice into the FOIA process to ensure the legal sufficiency review of the FOIA exemptions and redactions.

Based on a later response from KENNEDY, the Department of State had accepted recommendations number one and three. LINICK suggested the FBI talk to [redacted] and [redacted] who both worked at STATE IG. [redacted] and [redacted] would be able to give more insight into the FOIA review process, and STATE IG's interaction with Secretary Clinton's counsel, Williams & Connolly. LINICK believed [redacted] had sent emails back and forth with David KENDALL, Secretary Clinton's attorney.

b6  
b7C

LINICK surmised the Department of State Foreign Affairs Manual that was in use during Secretary Clinton's tenure as Secretary of State did not give clear and specific guidance regarding the use of private email, although it was highly discouraged. If employees used private email to conduct official State Department business, that email had to be forwarded to an @state.gov email within twenty days after being sent. The Department of State had no process for approving the use of private networks. There were no rules in place that specifically denied Secretary Clinton the use of her private network.

Continuation of FD-302 of Interview of Steve A. Linick, On 08/05/2015, Page 3

LINICK did not believe he was qualified to explain the Department of State's retroactive classification process. LINICK did not know whether the Department of State had provided a safe to Williams & Connolly, nor did LINICK know if the Department of State had the authority to certify a non-government facility as secure storage for classified information.

LINICK advised Secretary Clinton had brought Bryan PAGLIANO into the Department of State to set up her private network. PAGLIANO was still a Department of State employee who worked in the Department of State's information technology department. However, PAGLIANO refused to be interviewed by STATE IG. PAGLIANO informed STATE IG he was represented by counsel from Akin Gump Straus Hauer & Feld, LLP. LINICK recommended the FBI interview PAGLIANO.

LINICK did not intend on directly contacting Secretary Clinton to request electronic copies of her private network email. Since there was a spillage of classified information, for which STATE IG is not equipped to handle, the referral was made to the FBI.

Continuation of FD-302 of Interview of Steve A. Linick, On 08/05/2015, Page 4

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/02/2015

JUSTIN GREGORY COOPER, date of birth (DOB) [REDACTED] and social security account number (SSAN) [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED] at the law offices of [REDACTED] located at [REDACTED] Washington DC 20006. Also present for the interview were [REDACTED] attorneys [REDACTED] and [REDACTED] as well as attorney [REDACTED] U.S. Department of Justice and [REDACTED] Assistant United States Attorney for the Eastern District of Virginia. After being advised of the identity of the interviewing Agents, and the nature of the interview, COOPER provided the following information:

b6  
b7C

Before commencing the interview, COOPER's attorney [REDACTED] stated the offices of [REDACTED] were in possession of two (2) Apple MacBooks and one (1) Seagate external hard drive belonging to COOPER. COOPER used one of the MacBooks from approximately 2009 to 2013 and transferred his files to the second MacBook in approximately 2013. The Seagate external hard drive contained back-up files belonging to COOPER. On the foregoing digital media existed files related to the upgrade of former Secretary of State HILLARY CLINTON's BlackBerry, incurred while COOPER upgraded HILLARY CLINTON's BlackBerry device in 2009 and 2011. These files were separate, segregated and labeled in folders on each of COOPER's digital media as described above. Additionally, each of COOPER's digital media items contained email exchanged with an email address belonging to HILLARY CLINTON, HDR22@clintonemail.com. [REDACTED] indicated COOPER is willing to discuss providing the FBI the folder containing BlackBerry files relating to the upgrade of HILLARY CLINTON's device, and all email involving the email address HDR22@clintonemail.com. Additionally,

b6  
b7CInvestigation on 09/02/2015 at Washington, DCb3  
b7EFile # [REDACTED] 302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b6  
b7C

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 09/02/2015, Page 2

[REDACTED] indicated COOPER did not have the right to provide consent to search the foregoing BlackBerry files and to gain consent to search, [REDACTED] believed the FBI would need to consult HILLARY CLINTON's lawyers at WILLIAMS AND CONNOLLY.

b6  
b7C

COOPER stated he worked for former President BILL CLINTON for approximately 16 years as an aide serving many capacities. In 2007, COOPER and other aides debated using a private server for the sole purpose of email exchange and as a result, a contract with Apple was signed for the set-up and administration of an OS X server (hereafter, Apple server). The foregoing Apple server was installed at the CLINTON residence located in Chappaqua, New York and was online in and around June 2008 and configured for a handful of users. COOPER recalled [REDACTED]

b6  
b7C

[REDACTED] having email accounts using the domain presidentclinton.com. The domain wjcoffice.com was another domain used for BILL CLINTON related staff and email, but COOPER referred to it as a legacy domain that had mostly forwarded email. BILL CLINTON did not have an email account on the Apple server and did not use email as far as COOPER understood. In January 2009, HILLARY CLINTON was looking to move away from a BlackBerry with AT&T service, and decided to register the domain clintonemail.com and host it on the Apple server. COOPER had no specific memory, but believed he could have been the individual to register the domain because he handled financial issues for the CLINTONS. In or around January 2009, the users determined the Apple server was not robust enough and based this assessment on unreliable BlackBerry connectivity. At that time, the Apple server was not run in conjunction with a BlackBerry Enterprise Server (BES).

In or around March 2009, BRYAN PAGLIANO, an Information Technology (IT) professional used by HILLARY CLINTON, took full control of setting up a Windows Small Business Server (hereafter, Windows server) as well as a BES, at the CLINTON residence in Chappaqua, New York. PAGLIANO built the server from equipment used in HILLARY CLINTON's campaign for the democratic nomination to run for President of the United States. COOPER did not know where PAGLIANO built the server, but knew it was in place and running at the Chappaqua residence in or around March 2009. COOPER was aware that



Continuation of FD-302 of Interview of Justin Gregory Cooper, On 09/02/2015, Page 3

PAGLIANO set-up firewalls, spam filters and possibly Cisco Adaptive Security Appliance (ASA) software, but only PAGLIANO would know the configuration of the set-up. PAGLIANO managed the porting of users from the Apple server to the Windows server, as well as handled all software upgrades and general maintenance. COOPER believed there was a back-up drive as part of the Windows server and wasn't aware of any additional back-ups, although he recalled many boxes around the Windows server and reiterated PAGLIANO would know the exact configuration. Concerning the various avenues of connectivity to the server for user devices, COOPER referred Agents to PAGLIANO. Cablevision provided internet service to the CLINTON residence in Chappaqua, and that internet service was used to connect the Windows server. COOPER believed no outside spam service provider was retained for the Windows server. COOPER believed in instances where the Windows server went down, like in the event of a power outage, emails were re-directed to a gmail account as a back-up. COOPER was aware of two (2) power outages, based on storms or natural disasters, occurring during the lifecycle of the Windows server, but was not aware of any specific users or corresponding gmail accounts that had email forwarded.

COOPER was granted administrator rights, along with PAGLIANO, to the Windows server and described his role as the customer service face. As part of this role, COOPER could add a user or reset a password. COOPER also continued in his role of acquisition or purchasing for the CLINTONS, and this extended to server related items. For instance, COOPER recalled using both Network Solutions and GoDaddy to register domains, but would only have used these companies because he was directed to, either by Apple or PAGLIANO. COOPER read in the press about the Windows server being associated with a company called Perfect Privacy, and would not be surprised if it was accurate, but had no specific memory of using the company. COOPER registered a Secure Socket Layer (SSL) at PAGLIANO's direction and recalled it being used for more security when users accessed their email from various computers, and eventually, iOS devices. Additionally, COOPER vaguely recalled the Windows server using a Microsoft software product called Forefront.

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 09/02/2015, Page 4

COOPER stated there was no official security policy given to users of the Windows server. Generally, when users received suspicious emails and forwarded them to COOPER, he would forward them to PAGLIANO. As an administrator of the Windows server, COOPER would get emails indicating brute force attacks (BFA). COOPER would also forward those to PAGLIANO and recalled PAGLIANO installing Internet Protocol (IP) blocking software in an attempt to thwart the BFA. On at least two (2) occasions, COOPER remembers making [REDACTED] Special Agent in Charge, United States Secret Service, aware of suspicious email received on the Windows server.

b6  
b7c

COOPER recalled conversations between CHERYL MILLS and BRYAN PAGLIANO in or about June 2013 pertaining to the decommissioning of the Windows server and the next phase of communication infrastructure for HILLARY CLINTON, after her tenure as Secretary of State in 2013. Although COOPER wasn't involved and doesn't recall how they were selected, PLATTE RIVER NETWORKS (PRN) was chosen to maintain a server for the CLINTONS. COOPER did recall some communication with PRN regarding the transfer of user names and accounts from the Windows server to PRN. An individual employed by PRN named [REDACTED] Last Name Unknown (LNU) was granted administrator rights on the Windows server in order to effect the transition to PRN's control. At this point, Interviewing Agents displayed a document to COOPER identifying administrator accounts on the Windows server. COOPER identified the administrator account [REDACTED] as most likely being the user name for [REDACTED] LNU from PRN. In or around July 2013, COOPER received instructions for his email account that indicated PRN was in control of the Windows server email data. Due to COOPER's transition in employment, his email account was off the server in or around November 2013. COOPER does not know when the Windows server was shut down and how or where it was transported.

b6  
b7c

COOPER had no knowledge of the process HILLARY CLINTON undertook when acquiring her emails from the clintonemail.com domain and providing them to the Department of State as part of a Freedom of Information Act (FOIA) request. COOPER speculated that PRN was involved in the acquisition of the entire content of her account and DAVID KENDALL was consulted when determining which specific emails would be turned over.

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 09/02/2015, Page 5

COOPER believed the Windows server had three domains: wjcoffice.com, presidentclinton.com and clintonemail.com. To the best of COOPER's memory, he recalled [REDACTED]

b6  
b7c

[REDACTED] having email accounts using the domain presidentclinton.com or wjcoffice.com, as part of their work for BILL CLINTON. COOPER believed HILLARY CLINTON, [REDACTED] and HUMA ABEDIN had email accounts under the domain clintonemail.com as part of their association or work for HILLARY CLINTON. COOPER believed the Windows server was used exclusively for the exchange of email.

COOPER has never stored or transmitted classified information over an unclassified network and was unaware of any discussions regarding the transmittal of classified information on an unclassified network by others.

Notes of this interview, as well as the document displayed to COOPER, will be maintained in a FD-340 envelope and filed with the captioned investigation.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/04/2016

(U//~~FOUO~~) On March 2, 2016, JUSTIN GREGORY COOPER, date of birth (DOB) [REDACTED] and social security account number (SSAN) [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED] at the law offices of [REDACTED] located at [REDACTED] Washington DC 20006. Also present for the interview were [REDACTED] attorneys [REDACTED] and [REDACTED] as well as U.S. Department of Justice attorneys [REDACTED] and [REDACTED]. After being advised of the identity of the interviewing Agents, and the nature of the interview, COOPER provided the following information:

b6  
b7C

(U//~~FOUO~~) After reviewing an email referencing a new laptop for HILLARY CLINTON, COOPER recalled a Macbook Air purchased for CLINTON in the 2008 timeframe, but did not believe she ever used it. He did not recall the backup drive referenced in the email. The Macbook was likely purchased with a credit card because COOPER [REDACTED] to CLINTON's accounts and, therefore, had credit cards [REDACTED]. COOPER was not involved in the setup of the Macbook, but believed it was setup to access CLINTON's email. The intent was for CLINTON to use the Macbook in addition to her BlackBerry. In addition to COOPER, HUMA ABEDIN [REDACTED] and, later, MONICA HANLEY frequently assisted CLINTON with setting up any new technology devices.

b6  
b7C

(U//~~FOUO~~) COOPER was aware CLINTON had Sensitive Compartmented Information Facilities (SCIFs) in both her New York residence as well as her residence in the District of Columbia (DC). The SCIF at the DC residence [REDACTED] COOPER knew CLINTON to have access to the SCIF and knew ABEDIN was frequently there, but did not know if ABEDIN could access the SCIF when it was secured. COOPER did not have the combination to open the SCIF. The SCIF doors at both residences were not always secured, including times when CLINTON was not at the residences. When CLINTON became the Secretary of State, COOPER assisted the team from the United States Department of State (State) with questions regarding the communications infrastructure at the New York residence. Both residences had safes, home computers, secure Cisco phones, secure and non-secure fax, and secure video capabilities inside of the SCIF. COOPER was unaware of who would receive secure faxes when they were transmitted. The only individual at either residence COOPER believed to have a clearance was possibly [REDACTED] as a result of his time in the military.

b6  
b7CInvestigation on 03/02/2016 at Washington, DCFile # [REDACTED]-302 Date dictated N/Ab3  
b7EBy SA [REDACTED] SA [REDACTED]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 03/02/2016, Page 2

(U//~~FOUO~~) Leading up to the installation of the Apple Server, COOPER, for several reasons, identified a need to setup a private email server located at the CLINTON residence. Those reasons included:

- segregating different aspects of WILLIAM CLINTON's post-presidency activities
- separating politics from the work of the Clinton Foundation

- [REDACTED]  
President CLINTON's office and might attempt to gain physical access to the server if it was located in the office

- An outside vendor might not report a hack attempt

b6  
b7c

(U//~~FOUO~~) After a series of phone calls with Apple, COOPER contracted with Apple Business Services to setup a server, hereafter Apple Server, for handling email for a small number of users working in the office of President CLINTON. COOPER did not recall how he paid for the Apple Server, but he likely used a credit card. Apple installed the Apple Server in the basement of the New York residence, however, COOPER did not recall if he was present for the setup. The CLINTON family and the staff at the New York residence were the only individuals with physical access to the Apple Server. The Apple Server design included a backup to an internal RAID drive. Apple assisted COOPER with the setup of the wjcoffice domain on the Apple Server, but Apple did not have ongoing access to the Apple Server or its contents. COOPER was the only one with administrative access to the Apple Server initially; later, BRYAN PAGLIANO was given access to effect the transfer of data on the Apple Server to a Microsoft Exchange server, hereafter Exchange Server. COOPER did not assist in exporting any of the data or files to the Exchange Server, nor did he create any archives of clintonemail.com data. The decision was made to move to the Exchange Server because the Apple Server did not keep up with changing developments in technology and, eventually, users experienced problems with email delivery on their BlackBerry devices.

(U//~~FOUO~~) COOPER believed HILLARY CLINTON had an email account on the Apple server; however, ABEDIN did not have an account. CLINTON either came up with or approved the username HDR22 for her email address.

(U//~~FOUO~~) After reviewing an email fragment referencing a potential hack of the Apple Server, COOPER stated he could not recall any details and did not believe the hack was ever confirmed.

(U//~~FOUO~~) CLINTON obtained a new BlackBerry device whenever she had an issue with her device, such as a trackball failure, cracked screen, or the device was too heavy. When one of these issues occurred, whoever was working in close proximity to CLINTON would obtain a new device for her. COOPER believed HANLEY, [REDACTED] and [REDACTED] to be the individuals who procured new devices for CLINTON. He did not recall obtaining devices on eBay or similar outlets. COOPER sometimes

b6  
b7c

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 03/02/2016, Page 3

assisted others with completing the switch to a new device by leading them through the process of backing up data from the old device and transferring it to the new device. After these steps were complete, COOPER would activate the new device on the Apple Server or, later, the Exchange Server. The two BlackBerry backups previously provided to the FBI by COOPER were likely from situations where COOPER directly handled the transition between devices. In these cases, COOPER destroyed the old devices by breaking them in half or hitting them with a hammer.

(U//~~FOUO~~) After reviewing an email referencing the replacement of CLINTON and ABEDIN's SIM cards, COOPER stated he did not recall a process whereby users would regularly switch SIM cards in their mobile devices, nor did he recall why CLINTON and ABEDIN received new SIM cards in the specific situation referenced in the email.

(U//~~FOUO~~) After reviewing an email dated May 30, 2009, COOPER stated he could not recall any details regarding a new BlackBerry for CLINTON in that timeframe.

(U//~~FOUO~~) After reviewing an email regarding new security policies, COOPER stated Research In Motion (RIM), provided new tools on a regular basis to increase the security of BlackBerry devices. Typically, when a user switched to a new device, COOPER would implement an updated security policy on the device. As an example of a feature he would add to a security policy, COOPER stated he required users to enter a more complex password. Users on older devices would have the old security policy.

(U//~~FOUO~~) The iPads used by CLINTON were for reviewing email and other content. COOPER stated [REDACTED] advocated for CLINTON's use of an iPad. Regarding specific iPads, COOPER recalled an iPad mini and at least one iPad having a cellular data connection in addition to a wireless network connection. COOPER never set up any of the iPads and, therefore, had no information on Apple IDs, iCloud accounts, or device passwords. One of the iPads locked out CLINTON's email account on one of the servers when it attempted to connect using an old password. COOPER could not recall on which server this event occurred.

b6  
b7C

(U//~~FOUO~~) After reviewing an email dated July 26, 2010, with the subject line "Re: CC for hPad," COOPER confirmed [REDACTED] purchased an iPad for CLINTON on or about that date.

b6  
b7C

(U//~~FOUO~~) After reviewing a chart with the heading "202 [REDACTED]" COOPER stated he recognized the phone number as CLINTON's second phone number. CLINTON usually carried a flip phone with her BlackBerry because it was more comfortable to talk on. Additionally, CLINTON could use her BlackBerry while talking on the flip phone. COOPER did not recognize any of the specific phones displayed in the chart.

b6  
b7C

(U//~~FOUO~~) COOPER stated [REDACTED] and he utilized Google hosting services for email when there was a problem with the Apple Server or Exchange Server. To

b6  
b7C

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 03/02/2016, Page 4

effect this change, COOPER would alter the settings on a user's device to check Google for new messages. COOPER could not recall if CLINTON or ABEDIN utilized Google hosting services during Hurricane Sandy or other outages. If they had used Google, it would have been a team effort to set up their devices because COOPER was traveling at the time.

(U//~~FOUO~~) After reviewing emails regarding the transfer of an archive of HILLARY CLINTON's emails, COOPER stated he did not recall providing a laptop to HANLEY for this purpose, but it was conceivable he could have repurposed a laptop from President CLINTON's office and assisted in the transfer of the email files. COOPER did not recall a USB flash drive containing the email files. He also did not recall HANLEY returning the laptop in early 2014; however, he became a consultant to President CLINTON in the fall of 2013 and was no longer involved in day-to-day business by 2014.

(U//~~FOUO~~) COOPER had minimal contact with Platte River Networks (PRN). He recalled one interaction with [REDACTED] to pass along passwords, but did not have any other involvement with PRN. COOPER did not have an email account with President CLINTON's office after he became a consultant.

b6  
b7c

(U//~~FOUO~~) COOPER had no knowledge of Freedom of Information Act production or the cull down process, as it related to CLINTON's emails from her time as Secretary of State.

(U//~~FOUO~~) Notes of this interview, as well as the documents displayed to COOPER, are maintained in a FD-340 envelope and filed with the captioned investigation.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/24/2016

(U//~~FOUO~~) On June 21, 2016, JUSTIN GREGORY COOPER, date of birth (DOB) [REDACTED] and social security account number (SSAN) [REDACTED] was interviewed telephonically by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED]. Also on the call for the interview were [REDACTED] attorneys [REDACTED] and [REDACTED] as well as attorney [REDACTED] U.S. Department of Justice. After being advised of the identity of the interviewing Agents, and the nature of the interview, COOPER provided the following information:

b6  
b7C

(U//~~FOUO~~) COOPER recalled a personally-owned iMac computer in the Sensitive Compartmented Information Facility (SCIF) of both the Washington, DC and Chappaqua, NY residence of HILLARY CLINTON. Despite not knowing the exact model, COOPER described them as being identical models with a one inch thick monitor.

(U//~~FOUO~~) COOPER stated an Apple server was set-up for email exchange for aides working for former President WILLIAM CLINTON. COOPER did not recall a specific person deciding to set-up the server, but more a consensus among aides.

(U//~~FOUO~~) In or around December 2008, COOPER recalled having conversations with HUMA ABEDIN pertaining to HILLARY CLINTON moving away from an AT&T provided email account and establishing an email domain on the Apple server. COOPER and ABEDIN discussed a covert email domain versus a domain including the CLINTON name. ABEDIN "blessed off" on the @clintonemail domain name and COOPER registered the domain in January 2009. COOPER could not recall who created the handle of HILLARY CLINTON's email account hdr22@clintonemail.com, but thought she typically approved her email account names. COOPER did not know if anyone else had HILLARY CLINTON's email account password, but stated if anyone would, it would be ABEDIN.

---

Investigation on 06/21/2016 at Washington, DCb3  
b7EFile # [REDACTED]-302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.



Continuation of FD-302 of Interview of Justin Gregory Cooper, On 06/21/2016, Page 2

(U//~~FOUO~~) COOPER did not have a specific memory of registering HILLARY CLINTON's email domain and setting up her clintonemail.com account on the Apple server. Most likely, COOPER believed he registered the domain, and added HILLARY CLINTON's email account to the Apple server, because he could think of no one else that would have performed that task. COOPER stated he most likely initially set HILLARY CLINTON's hdr22@clintonemail.com account to forward to her BlackBerry. When HILLARY CLINTON would reply from her BlackBerry, her email address would represent as hdr22@clintonemail.com. With that configuration, HILLARY CLINTON's incoming email content would have resided on the Apple server for a period of time, but not her sent messages. Again, COOPER stated this was "all a blur" to him and he was relaying the most likely scenario.

(U//~~FOUO~~) In early 2009, COOPER recalled conversations with ABEDIN regarding moving to another email server system, but could not recall specifics. COOPER recalled ABEDIN knew BRYAN PAGLIANO from his work on CLINTON's 2008 presidential campaign and held him in high regard. PAGLIANO began building a new email server system in early 2009. PAGLIANO had to have been given access to the Apple server in order to migrate email accounts and content to the new server he built. COOPER did not recall giving PAGLIANO administrator access to the Apple Server.

(U//~~FOUO~~) COOPER did not specifically recall acquiring an Apple computer for HILLARY CLINTON to use in April 2009. In general, COOPER recalled multiple attempts to get CLINTON to use Apple products.

(U//~~FOUO~~) Around January 2011, COOPER recalled receiving numerous alerts in his email indicating email account users of PAGLIANO's server were entering the wrong log-in credentials. PAGLIANO had set-up the server so that COOPER would receive failed log-in notifications. COOPER thought this to be a brute force attack on the server and contacted PAGLIANO. COOPER recalled nothing else regarding this incident.

(U//~~FOUO~~) COOPER recalled HILLARY CLINTON's email account was changed to hrc117@clintonemail.com after SIDNEY BLUMENTHAL's email account was hacked around March 2013. Although COOPER could not be

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 06/21/2016, Page 3

certain, COOPER thought he could have been the one to change the email address for CLINTON.

(U//~~FOUO~~) COOPER thought PAGLIANO had disabled the built-in Administrator account on the server PAGLIANO built. COOPER had his own system administrator account on PAGLIANO's server.

(U//~~FOUO~~) In order for Platte River Networks (PRN) to begin administering an email server for the CLINTONS, PAGLIANO gave [REDACTED] access to PAGLIANO's server. COOPER was unsure when this took place, but thought it was in May or June of 2013. COOPER did not know if [REDACTED] removed COOPER's administrator account.

b6  
b7c

(U//~~FOUO~~) COOPER could not recall when he last logged into PAGLIANO's server. COOPER did not know what "IP scanning tools" were.

(U//~~FOUO~~) In the spring of 2013, COOPER recalled giving MONICA HANLEY a MacBook laptop and walking her through downloading CLINTON's email from the PAGLIANO server to the MacBook. COOPER did not recall a specific purpose for this other than maintaining a back-up copy of CLINTON's email. COOPER was unaware of a USB Flash Drive containing CLINTON's email. COOPER was unaware of the location of the MacBook containing CLINTON's email.

(U//~~FOUO~~) COOPER stated [REDACTED] did not have access to the Apple server in anyway.

b6  
b7c

(U//~~FOUO~~) Notes of this interview will be maintained in a FD340 envelope and filed with the captioned investigation.

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/23/2016

(U//~~FOUO~~) On February 19, 2016, ERIC J. BOSWELL, DOB [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at the law offices of [REDACTED] Washington DC. Also present for the interview was BOSWELL's attorney [REDACTED]. After being advised of the identities of the interviewing agents, and the purpose of the interview, BOSWELL provided the following information:

b6  
b7C

(U//~~FOUO~~) BOSWELL served as the United States Assistant Secretary for State for Diplomatic Security (DS) from June 2008 until December 2012, however, BOSWELL did not resign from DoS until the Fall of 2013. Following his resignation from Department of State (DoS), BOSWELL went into "When Actually Employed" (WAE) status with DoS, which essentially means he still works for and is paid by DoS on an as needed basis.

(U//~~FOUO~~) As the Assistant Secretary of State for Diplomatic Security, BOSWELL was responsible for overseeing the security of DoS communications, personnel, and programs.

(U//~~FOUO~~) BOSWELL did not directly oversee the security of the Executive Secretariat, to include former Secretary of State HILLARY R. CLINTON. A Security Officer who reported further down in BOSWELL's chain of command had direct oversight over the Executive Secretariat on the seventh floor offices commonly referred to as "Mahogany Row." BOSWELL could not recall the names of any of the Security Officers who were assigned to Mahogany Row during his tenure.

(U//~~FOUO~~) BOSWELL had no knowledge CLINTON was using a personal email, nor that she was operating said email off of a personal server while she was Secretary of State. He first learned of the private server and personal email use when it was reported in the Press. BOSWELL further stated he found former Secretary CLINTON to be "very responsive to security issues."

(U//~~FOUO~~) Agents asked BOSWELL to review a redacted memo titled "Use of Blackberries in Mahogany Row." The memo was redacted by DoS in response to a Freedom of Information Act (FOIA) inquiry. After reviewing the memo, BOSWELL stated the memo was drafted early in the Administration, and shortly after CLINTON began her tenure at DoS.

Investigation on 2/19/2016 at Washington, DC

File # [REDACTED]-302 Date dictated N/A

By SA [REDACTED] SA [REDACTED]

b3  
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

Continuation of FD-302 of Interview of Eric J. Boswell, On 2/18/2016, Page 2

(U//~~FOUO~~) BOSWELL recalled CLINTON's DoS executive staff initially inquiring about the possibility of acquiring Blackberries that could be configured for classified material. BOSWELL, tasked his staff to research the request and possibilities. BOSWELL staff notified him that such a device/configuration was not possible, which was relayed to CLINTON's executive team via the memo.

(U//~~FOUO~~) Furthermore, BOSWELL stated that he recalled there was general concern around the same time regarding the possibility that CLINTON's staff might use their Blackberries on Mahogany Row, which is a Sensitive Compartmented Information Facility (SCIF). According to BOSWELL there was no specific instance or report that any specific person/people were using Blackberries on Mahogany Row at the time. However, there was some general concern within DoS security personnel that CLINTON's executive staff may try to use their Blackberries in the SCIF as they were almost all brought on to DoS from CLINTON's campaign team, and thus were very accustomed to using their Blackberries. Although BOSWELL could not recall a specific report of the use of Blackberries on Mahogany Row, he stated that "they were told to stop (using their Blackberries in the SCIF) and they did." DS never sanctioned the use of Blackberries on Mahogany Row.

(U//~~FOUO~~) Agents also asked BOSWELL to review a redacted email dated 1/24/2009 with the subject line "Series of questions." The email exchange, which BOSWELL was not copied on, related to the set up of a "stand-alone separate network PC" for CLINTON. In response, BOSWELL stated the email was written three days after CLINTON began her tenure as Secretary of State. LEWIS "Lou" LUKINS who was included in the referenced email exchange, was the former Chief Administrative Officer of the Executive Secretariat. BOSWELL explained that a "stand alone" work station does not necessarily mean a workstation that was not connected to the DoS network, and it just referred to a normal computer workstation. BOSWELL was unsure if CLINTON ever used a workstation at DoS, and did not recall ever seeing a workstation in her office.

(U//~~FOUO~~) A copy of the original interview notes and the referenced memo are attached in a 1A envelope.

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/17/2016

(U//~~FOUO~~) On June 15, 2016, LEWIS LUKENS, Date of Birth [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at his residence, [REDACTED] San Francisco, CA. After being advised of the identities of the interviewing agents, and the purpose of the interview, LUKENS provided the following information:

b6  
b7c

(U//~~FOUO~~) LUKENS is currently the Diplomat in Residence for the Pacific Northwest region of the US, for the US Department of State (DOS). LUKENS, a career DOS employee, was most recently the US Ambassador to Senegal, before which he was the Deputy Assistant Secretary of State for the Executive Secretariat. As the Deputy Assistant Secretary, from the summer of 2008 until June of 2011, LUKENS reported to the Executive Secretariat, who was initially DAN SMITH until he was succeeded by STEPHEN MULL. LUKENS was responsible for providing operational and logistical support to approximately 800 individuals at the DOS, which included the Secretary of State, senior leadership and their staff. LUKENS responsibilities were broken into five main areas: Human Resources, Budget, General Services, Diplomatic Security (DS), and Information Resource Management (S/ES - IRM).

(U//~~FOUO~~) S/ES - IRM was responsible for ensuring that the senior leadership of DOS had the Information Technology (IT) tools and systems they needed to do their jobs. The group was led by JOHN BENTEL and was comprised of approximately 25 to 30 individuals who were a mix of DOS personnel and contractors. LUKENS interacted with BENTEL on a daily basis. He described BENTEL as having "decent [technical] skills" despite not being a "tech guy" and added that he was more technically proficient than LUKENS was. LUKENS was not aware of the statements that had been attributed to BENTEL in the recent OIG report, but thought they were out of character for BENTEL.

(U//~~FOUO~~) LUKENS worked with CHERYL MILLS and HUMA ABEDIN before and during HILLARY CLINTON's transition to DOS to coordinate CLINTON's office space and human resource needs. LUKENS explained that the previous Secretary only had one Deputy Secretary but CLINTON planned to have two Deputies, so LUKENS had to reorganize the offices on the 7<sup>th</sup> floor to accommodate the second Deputy. LUKENS worked with DAN SMITH and Under Secretary PATRICK KENNEDY at DOS to ensure that CLINTON's needs were met during the transition. LUKENS stated there was not a computer in CLINTON's office at DOS because CONDOLEEZZA RICE did not have one, and one was not installed for CLINTON.

(U//~~FOUO~~) LUKENS and representatives from DS and S/ES-IRM visited CLINTON's residence in Washington, DC during the transition to assess what equipment was present and what needed to be

Investigation on 6/15/2016 at San Francisco, CA

b3  
b7E

File # [REDACTED] 302 Date dictated N/A

By SA [REDACTED] SA [REDACTED]

b6  
b7c

Continuation of FD-302 of Interview of Lewis Lukens, On 6/15/2016, Page 2

installed. LUKENS provided that both secure and unsecure telephone and facsimile systems were installed at the residence. LUKENS did not recall if there was a computer in the Washington residence. LUKENS did not visit CLINTON's residence in Chappaqua, NY and instead sent [REDACTED] in his place. LUKENS was not aware of what equipment was installed in Chappaqua. LUKENS stated that the DS representative for these visits was mostly likely [REDACTED] who was later replaced by [REDACTED] in the summer of 2009.

b6  
b7C

(U//~~FOUO~~) LUKENS was shown an email with the subject "State Department Telephone Services at Secretary Clinton's Residence" that was sent from [REDACTED] to LUKENS and ABEDIN on January 27, 2009. After reviewing the email, LUKENS explained that "IST/Red Switch" refers to the direct phones to the White House, "Business Lines" refers to unclassified phone lines, and "Ops Dedicated Drop" refers to a phone line that connected directly to the DOS operations center. LUKENS was not sure what "CMS VoIP" referred to but thought it was related to DOS Crisis Management Support. LUKENS noted that equipment was installed both in a SCIF and in an office area located near [REDACTED]. LUKENS stated that he oversaw the installation of the telephone lines in a very broad sense but the actual work was very technical and beyond his expertise.

b6  
b7C

(U//~~FOUO~~) [REDACTED] equipment. LUKENS described [REDACTED] as likeable but noted that he often interacted directly with CLINTON's staff and did not always keep his chain of command informed of requests from, and work begin done for, CLINTON and her team.

b6  
b7C

(U//~~FOUO~~) LUKENS was shown an email with the subject "Secretary Residential Installation Hotwash" that was sent from [REDACTED] to BENTEL, [REDACTED] and [REDACTED] on March 17, 2009. LUKENS was not immediately familiar with the email or the attachment but believed that "Server: Basement Telephone Closet" referred to a telephone server. LUKENS noted the installation processes was unique because there was pre-existing equipment in the residences that had previously been installed for President WILLIAM CLINTON.

b6  
b7C

(U//~~FOUO~~) LUKENS was not aware that CLINTON was using a private email server until it was released in the papers. Upon learning about the server, LUKENS had some general concerns about how the server had been protected from hackers. LUKENS did not know if the setup was a violation of any existing DOS policy at that time. LUKENS never had any conversations with CLINTON's staff or other department officials about the server.

(U//~~FOUO~~) LUKENS was shown an email with the subject "HRC blackberry" that was sent from MONICA HANLEY to ABEDIN on August 30, 2011. After reviewing the email, LUKENS provided that he was unaware of the email and that BENTEL never relayed any information to him about the server or it being nonfunctional.

(U//~~FOUO~~) LUKENS was shown an email with the subject "S Communications" that was sent from ABEDIN to MULL on August 30, 2011. LUKENS was familiar with the email and provided the

Continuation of FD-302 of Interview of Lewis Lukens, On 6/15/2016, Page 3

context that the technology at DOS was not very user friendly and that matters were further complicated because CLINTON was not very technology savvy and had little patience for technology issues.

(U//~~FOUO~~) LUKENS was shown an email with the subject "Re: Series of questions" that he sent to KENNEDY on January 24, 2009. LUKENS was familiar with the email and explained that CLINTON could not have her BlackBerry in the SCIF so his idea was to set up a living room area outside of the SCIF where CLINTON could check her emails on her BlackBerry. CLINTON did not have a computer in her office and did not want one because she preferred to use her BlackBerry for checking her emails. While DOS users can check personal email accounts via the unclassified DOS computer systems the proposed 'stand alone' system would have streamlined the process for CLINTON and would have been similar to the setup used by former Secretary of State COLIN POWELL.

(U//~~FOUO~~) LUKENS was aware that no DOS email account was assigned to CLINTON, aside from a generic account that was used for sending mass emails to DOS employees on behalf of the Secretary. LUKENS was not aware that CLINTON was using a personal email for official business. He was told by MILLS that CLINTON was using her personal account to keep in touch with friends and family. LUKENS did not email with CLINTON directly and typically communicated with ABEDIN, who he described as CLINTON's gatekeeper.

(U//~~FOUO~~) LUKENS was shown an email with the subject "Re: E-mail test" that was sent from HUMA to "H" on February 27, 2010. LUKENS was unaware of the issues discussed in the email exchange at that time, but he had since seen the email exchange. LUKENS stated that [REDACTED] who worked in BENTEL's group.

b6  
b7c

(U//~~FOUO~~) LUKENS was shown an email with the subject "Re: S berry" that was sent from HANLEY to ABEDIN on August 30, 2011. After reviewing the email LUKENS provided that he had not seen the email before and did not know the circumstances in which it was sent. LUKENS did not know why BENTEL made the statement regarding FOIA searches in the email.

(U//~~FOUO~~) LUKENS had heard of the State Messaging and Archive Retrieval Toolset (SMART) but was not aware of any specifics about the program. LUKENS believed that SMART had been rolled out to all departments at DOS and was not aware that it wasn't used by S/ES – IRM.

(U//~~FOUO~~) Once CLINTON's transition to DOS was completed LUKENS' primary responsibility became coordinating the travel logistics for CLINTON and her team. This included handling matters related to passports, customs / immigration requirements, baggage, and hotel arrangements. LUKENS travel on all of the trips with CLINTON.

(U//~~FOUO~~) LUKENS was shown an email with the subject "Communications Guidance for Moscow" the he sent to several individuals on CLINTON's staff on March 15, 2010. LUKENS did not recall receiving country specific threat briefs prior to each trip. However, LUKENS recounted that on one trip to Russia they received guidance from the Embassy that they should leave their phones on the plane.

Continuation of FD-302 of Interview of Lewis Lukens, On 6/15/2016, Page 4

However, this conflicted with the guidance from DS so they ultimately elected to take their phones off of the plane. LUKENS explained that the one.state.gov system referenced in the email was used for accessing the DOS OpenNet system remotely using a user specific pin and token.

(U//~~FOUO~~) A copy of the original interview notes and referenced documents are attached in a 1A envelope.



-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 4/07/2016

(U//~~FOUO~~) On April 5, 2016, HUMA ABEDIN, DOB [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at the FBI Washington Field Office, 601 4<sup>th</sup> Street NW, Washington DC. Present for the interview was ABEDIN's counsel, MIGUEL RODRIGUEZ, Partner at Bryan Cave LLP, KAREN DUNN, Partner at Boies, Schiller & Flexner LLP and [REDACTED] Associate at Boies, Schiller & Flexner LLP. Also present was FBI Section Chief Peter Strzok, as well as [REDACTED] Assistant U.S. Attorney – Eastern District of Virginia, and David Laufman, [REDACTED] and [REDACTED] from the Department of Justice (DoJ) Counterintelligence and Export Control Section. Prior to the interview RODRIGUEZ, DUNN and [REDACTED] agreed to sign a non-disclosure agreement in anticipation of viewing classified documents during the interview. After being advised of the identities of the interviewing agents, and the purpose of the interview ABEDIN provided the following information:

b6  
b7C

(U//~~FOUO~~) ABEDIN first met HILLARY R. CLINTON in 1996 when she was an intern in the Office of the First Lady. She then worked on CLINTON's Senate campaign and her 2008 Presidential campaign, as the traveling Chief of Staff. When CLINTON became the Secretary of State, at the Department of State (DoS), ABEDIN became her Deputy Chief of Staff for Operations where she was primarily responsible for coordinating logistics for CLINTON. ABEDIN worked with JAKE SULLIVAN, CHERYL MILLS, JOE MACMANUS, as well as three Special Assistants, a Scheduler, and a Personal Assistant while she was in the Office of the Secretary.

**Transition to Department of State**

(U//~~FOUO~~) ABEDIN and CLINTON met with DoS on a few occasions prior to CLINTON being sworn into office to discuss her transition. During these instances CLINTON and ABEDIN met with Secretary Rice and her staff to discuss the logistics of the transition. ABEDIN worked with PATRICK KENNEDY and MILLS to fill the available spots on CLINTON's staff. ABEDIN was directly responsible for identifying and interviewing individuals for the roles of Personal Assistant, Scheduler and Personal Correspondent.

(U//~~FOUO~~) ABEDIN provided that KENNEDY was their main point of contact for setting up CLINTON's office and that LEWIS LUKENS, MACMANUS and [REDACTED] were responsible for coordinating the technical aspects of the transition. ABEDIN did not know that CLINTON had a private

b6  
b7CInvestigation on 4/05/2016 at Washington, DCFile # [REDACTED]-302 Date dictated N/ABy SA [REDACTED] bh SA [REDACTED]b3  
b7Eb6  
b7C

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 2

server until about a year and a half ago when it became public knowledge and did not recall any discussion about it during the transition. ABEDIN did not recall any discussions during the transition about whether using a private email account for DoS business was permissible. However, she did recall that they were advised that they could not have personal emails linked to a DoS device. As a result CLINTON elected to use a personal device only because she did not want to carry two devices.

(U//~~FOUO~~) ABEDIN had never held a security clearance prior to working at DoS. She received a Top Secret security clearance at DoS but did not remember being read into any Special Access Programs (SAPs) or compartments. When ABEDIN was on boarded at DoS she received a security briefing that detailed the different levels of classified information and the proper handling procedures. ABEDIN did not recall ever receiving any training on the preservation of federal records but noted that she took a lot of training courses when she on boarded so she may have had training on the topic. ABEDIN provided that she was not an Original Classification Authority (OCA) at DoS.

#### **ABEDIN's Devices and Communication Practices**

(U//~~FOUO~~) ABEDIN's office was located in a Sensitive Compartmented Information Facility (SCIF) at DoS. At her desk she had both an unclassified and classified computer system. ABEDIN was not sure if the classified computer system was a Secret or Top Secret (TS) system, and she was unfamiliar with the term JWICS. ABEDIN did not receive any formal guidance on what system she should use for the different aspects of her work. She did the majority of her work on the unclassified system and would often go several days, or weeks, at a time without logging into her classified system. She would only use the classified system if she was notified that somebody had sent her a message on that system. In addition to the computer systems, ABEDIN had an open line phone and a yellow TS Cisco phone that she typically used for talking with the National Security Council.

(U//~~FOUO~~) ABEDIN provided that she was issued an official DoS email account, abedinh@state.gov, which she used for DoS related work. She also had an email account that was provided by CLINTON, huma@clintonemail.com, which she used for matters related to CLINTON's personal affairs and to communicate with CLINTON's personal staff and friends. ABEDIN also had a personal Yahoo email account, [REDACTED] ABEDIN could access her clintonemail.com account and her Yahoo account via the internet on the unclassified DoS computer system. She would use these accounts if her DoS account was down or if she needed to print an email or document. ABEDIN further explained that it was difficult to print from the DoS system so she routinely forwarded emails to her non-DoS accounts so she could more easily print. ABEDIN also had another email account that she had previously used to support her husband's campaign activities, [REDACTED]

b6  
b7c

(U//~~FOUO~~) ABEDIN had no knowledge of her accounts ever being targeted by hackers and was not aware of any intrusion attempts. ABEDIN recalled that some people at DoS had issues with their Gmail accounts but she never had a Gmail account.

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 3

(U//~~FOUO~~) ABEDIN was shown an email dated September 1, 2011, with the subject "Fwd: Calls", which she forwarded from her huma@clintonemail.com account to her DoS email account. ABEDIN did not recall the specific email or why she would have forwarded it. However, she noted that based on the date stamp she knew that she was not in the office when it occurred.

(U//~~FOUO~~) ABEDIN was shown an email dated October 4, 2009, with the subject "Fwd: U.S. interest in Pak Paper 10-04", which ABEDIN received from [REDACTED] and then forwarded to her Yahoo email account. ABEDIN was not familiar with the document but was not surprised that she forwarded it to her Yahoo account. She explained that she routinely forwarded emails from her state.gov account to either her clintonemail.com or her yahoo.com account so that she could print them. ABEDIN stated that she would typically print the documents without reading them. At the time of the email, [REDACTED] worked for RICHARD HOLBROOKE who was the Special Representative for Afghanistan and Pakistan (SRAP). ABEDIN was unaware of the classification of the document and stated that she did not make judgments on the classification of material that she received. Instead, she relied on the sender to make that assessment and to properly mark and transmit the document.

b6  
b7C

(U//~~FOUO~~) ABEDIN was shown an email chain dated August 16, 2010, with the subject "Re: your yahoo acct". ABEDIN did not recall the email and provided that despite the content of the email she was not sure that her email account had ever been compromised. She further provided that the [REDACTED] referenced in the email referred to [REDACTED] an older campaign volunteer in Westchester, NY.

b6  
b7C

(U//~~FOUO~~) ABEDIN was provided with a DoS Blackberry and believed that all of CLINTON's top aides at DoS were issued Blackberries as well. The team would sometime use secure cell phones when they were traveling but they were not used on every trip. Secure phones were only used when traveling in hostile operational environments. The secure phones were maintained by Diplomatic Security (DS) and would be provided to the team by [REDACTED] ABEDIN provided that DS routinely provided country specific security briefings prior to international trips. During these briefings the team would receive instructions on how to handle their communications once in country. For example the team might be told to leave their phones on the plane or to take the batteries out of their phones. ABEDIN noted that the guidance changed based on the specific location and that it wasn't uncommon to receive different instructions on separate trips to a given country. For example, the communication plan for Moscow could be different than the plan in St. Petersburg.

b6  
b7C

(U//~~FOUO~~) ABEDIN was shown an email chain dated October 6, 2009, with the subject "IT security in Moscow" and an email chain dated October 12, 2009, with the subject "Re: Communications". ABEDIN stated that the content of these emails was typical of the guidance that was provided by DS prior to a trip and that the instructions were closely followed by the traveling team. If CLINTON was not able to attend the DS briefing prior to the team's departure she would be briefed by DS on the plane. ABEDIN stated that they used computers that were set up and controlled by the Mobile Communications Team to access their DoS and personal emails accounts when they were in Russia.

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 4

(U//~~FOUO~~) ABEDIN did not recall any potential security issues occurring while the team was traveling overseas aside from one instance in Egypt. Prior to a meeting at President Mubarak's residence, the team was unexpectedly asked to leave their phones. ABEDIN could not provide any more details on what had occurred but noted that DS was with the team and was aware of the incident.

### **The Secretary's Devices and Practices**

(U//~~FOUO~~) CLINTON's office at DoS was located in a SCIF on the seventh floor that was commonly referred to as Mahogany Row. Her office had an unclassified telephone and a TS Cisco phone for contacting other agencies. Initially, she also had a secure 'white phone' and a STE in her office but they were later removed. CLINTON did not have a computer in her office and conducted the majority of her work in person or on paper. ABEDIN explained that CLINTON could not use a computer and that she primarily used her Blackberry or iPad for checking emails. If CLINTON needed to check her emails during the course of the day she would leave the SCIF to check her Blackberry, often going to the eighth floor balcony. CLINTON's email address was not widely known but all of her senior staff had the address and would share it with other government officials if they needed it. ABEDIN stated that CLINTON's senior staff was not specifically instructed to filter her email but they understood what was relevant to CLINTON and would only share information with her as appropriate.

(U//~~FOUO~~) ABEDIN was shown an email chain dated September 30, 2010, with the subject "Re: HbJ on moratorium". After reviewing the email, ABEDIN could not recall the email exchange or the context of the email. ABEDIN stated that, in general, she would be told by either CLINTON or the requesting party if the call needed to be secure or not. It would be unusual for ABEDIN to read the content and then make her own judgment as to whether the call should be secure or not. ABEDIN stated that she was likely with CLINTON when she sent the email and she was relaying guidance from CLINTON. ABEDIN provided that [REDACTED] and [REDACTED] were assistants to CLINTON.

b6  
b7c

(U//~~FOUO~~) ABEDIN was shown an email chain dated August 30, 2011, with the subject "Re: S Communications". ABEDIN recalled the email exchange and provided that CLINTON was not issued a DoS Blackberry and that she only used her personal Blackberry because she did not want to carry multiple devices. The email exchange occurred when CLINTON was in the Hamptons and was having communication issues following Hurricane Irene. At that time, ABEDIN felt that it did not make sense to temporarily issue CLINTON a DoS Blackberry because it would require significant effort to transfer all of her emails and contacts to a device that she would only use for a few days. ABEDIN did not know what STEPHEN MULL meant when he wrote that the account could be set up to mask CLINTON's identity. ABEDIN's counsel noted that a longer version of this email chain had been released via the FOIA process (DoS case F-2015-12685, document C05905671).

(U//~~FOUO~~) ABEDIN was shown a memorandum from DS regarding the use of Blackberries in Mahogany Row. ABEDIN recalled seeing the memorandum in the news recently but did not recall when it was originally released. ABEDIN stated that she did not need her Blackberry when she was in the SCIF

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 5

so she was not affected by the recommendations in the memorandum. ABEDIN did not remember receiving a specific briefing from DS on Blackberry vulnerabilities but stated that it was possible that she received one because DS frequently briefed CLINTON's team on security topics.

(U//~~FOUO~~) CLINTON did not have a secure Blackberry and ABEDIN did not know if secure Blackberries were even available at that time. ABEDIN stated that CLINTON had several different standard Blackberry phones during her tenure. It wasn't uncommon for CLINTON to use a new Blackberry for a few days and then immediately switch it out for an older version that she was more familiar with. The phones were typically purchased by somebody on her staff and would be activated by "whoever was around". ABEDIN recalled that [REDACTED] and MONICA HANLEY helped to setup new Blackberries on different occasions. ABEDIN did not know what was done with the old Blackberries after CLINTON transitioned to a new one. ABEDIN was shown an email chain dated April 15, 2009, with the subject "Re: Won't get to huma today". ABEDIN did not recall why they were activating new SIM cards for CLINTON. ABEDIN provided that [REDACTED] [LAST NAME UNKNOWN] was [REDACTED] President Clinton's office that may have worked for JUSTIN COOPER.

b6  
b7c

(U//~~FOUO~~) ABEDIN confirmed that CLINTON's Blackberry phone number was 212 [REDACTED]. She was not aware of CLINTON ever using a second cell phone and was not familiar with the phone number 202 [REDACTED]. [It is noted that a 202 area code was erroneously used when ABEDIN was asked about the aforementioned telephone. The correct number is 212 [REDACTED]. While ABEDIN noted that it would be odd for CLINTON to have a D.C. area code, she ultimately stated that no part of the number was familiar to her].

b6  
b7c

(U//~~FOUO~~) ABEDIN stated that CLINTON had at least one, or possibly two, iPads during her tenure. She believed that one of them might have been a gift. CLINTON used the iPad for reading news articles but ABEDIN rarely saw CLINTON carrying or using the iPad. CLINTON was trained on how to use the iPad by [REDACTED] while they were on traveling on a plane. ABEDIN stated that the iPad was briefly used to send and receive emails following Hurricane Irene when CLINTON's other email systems were down. Although this was only intended as a temporary solution, this capability may have remained after CLINTON's other systems were restored. ABEDIN noted that she was in Europe when Irene struck and that HANLEY was responsible for handling the communication issues following the storm. ABEDIN confirmed that CLINTON's email was also down for an extended period of time following Hurricane Sandy. However, ABEDIN was in New York City, with her infant child, at the time and was not sure what efforts were taken to restore or establish temporary email for CLINTON. ABEDIN was unaware of any email accounts, Apple IDs, or cloud storage accounts associated with the iPads.

b6  
b7c

### Email System During Tenure

(U//~~FOUO~~) ABEDIN contacted COOPER about getting a Blackberry for CLINTON while CLINTON was still in the Senate. CLINTON then used the Blackberry when she transitioned to DoS. At that time, her primary email address was hr15@att.blackberry.net. Shortly after CLINTON became the Secretary of State COOPER established the @clintonemail.com domain and CLINTON began using

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 6

hdr22@clintonemail.com as her primary email. The only other person at DoS to receive an email account on the domain was ABEDIN. Later in CLINTON's tenure she changed her email address to hrod17@clintonemail.com. ABEDIN was not familiar with the email address hr15@mycingular.blackberry.net or with [REDACTED]@gmail.com.

b6  
b7c

(U//~~FOUO~~) Initially COOPER was the primary point of contact for anything related to the setup and maintenance of the email system. ABEDIN was shown three separate email chains with COOPER regarding the operation of the server during CLINTON's tenure. The first was sent on January 9, 2011 and had the subject "Re:", the second was sent January 10, 2011 and had the subject "Don't email hrc anything sensitive. I can explain more in person" and the third was sent October 20 2011 and had the subject "Re:". ABEDIN provided that she did not recall any details surround these email exchanges but noted that she trusted COOPER to fix any issues with the server. She did not recall the system ever being hacked but assumed that she would have notified CLINTON of any current issues that they were experiencing.

(U//~~FOUO~~) ABEDIN was shown an email chain dated March 17, 2011 with the subject "Re: School". Upon reviewing the email she provided that she was not familiar with the email or the topics discussed within it. ABEDIN noted that her email address was misspelled on the chain and therefore she would not have received the email. However, she was not aware of the @clintonemail.com system ever being hacked.

(U//~~FOUO~~) ABEDIN provided that BRYAN PAGLIANO had worked on the Information Technology (IT) team for CLINTON's 2008 Presidential campaign and was hired at DoS after CLINTON took office. Thereafter, BRYAN PAGLIANO became the new point of contact for issues with the email system. ABEDIN did not specify when this occurred but stated that there was a transition period during which she would contact COOPER and he would direct her to contact PAGLIANO.

(U//~~FOUO~~) ABEDIN was shown an email chain dated December 24, 2012, with the subject "Fw: Thank You". After reviewing the emails ABEDIN provided that she did not recognize the SMSGS@state.gov email address and was not aware of any other generic email accounts used by CLINTON for DoS wide email communications.

(U//~~FOUO~~) ABEDIN was shown an email chain dated August 30, 2011, with the subject "Re: S berry". ABEDIN stated that she did not like the SSHRC@state.gov email address because it was too obvious of an email address. She noted that the email appeared to be related to discussions that occurred when they were working to restore CLINTON's communications after Hurricane Irene. ABEDIN did not know who JOHN A. BENTAL was but assumed that he worked in the IT department at DoS. When asked about BENTAL's statement that SSHRC@state.gov would be subject to FOIA searches, ABEDIN stated that she always assumed that all of CLINTON's communications, regardless of the account, were subject to FOIA if they contained related material. ABEDIN did not recall ever having conversations with CLINTON, or any other staff members, about the Federal Records Act and preserving relevant emails.

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 7

ABEDIN provided that at the time, they believed relevant emails would be captured and preserved by DoS if any of the senders or recipients were using an official DoS email account.

(U//~~FOUO~~) ABEDIN was shown an email chain dated December 16, 2010, with the subject "RE: mail from clintonemail". ABEDIN recalled that there had been a problem with emails from the @clintonemail.com system being filtered out by the DoS email system, but she did not recall the specific email exchange. ABEDIN noted that it appeared that it was SULLIVAN's emails that were affected and that it would otherwise be uncommon for him to be involved in discussions about email issues.

### Email System Post Tenure

(U//~~FOUO~~) Following CLINTON's tenure at DoS she established a personal office in New York City for the purpose of writing her book and pursuing other interests. Several members of CLINTON's staff from DoS joined CLINTON's team in New York. They included: ABEDIN, HANLEY, [REDACTED] [REDACTED] and [REDACTED] [believed to be [REDACTED]] also continued to support CLINTON on a limited basis as consultants.

b6  
b7C

(U//~~FOUO~~) When CLINTON's team was formed, [REDACTED] established temporary Gmail accounts for members of the team using the naming convention hrco@gmail.com. [REDACTED] had been CLINTON's [REDACTED] at DoS and ABEDIN described him as being good with technology. He set up the email accounts for the team so that they would have something more formal than their personal emails accounts.

b6  
b7C

(U//~~FOUO~~) When CLINTON left DoS she stopped using the clintonemail.com system and started using hrcoffice.com to formalize her transition. During this same time period, an outside IT company, PLATTE RIVER NETWORKS (PRN), was hired to maintain CLINTON's email system. ABEDIN stated that PRN was initially hired to manage President CLINTON and [REDACTED] emails. It was then later decided that PRN should also manage CLINTON's email as well.

b6  
b7C

(U//~~FOUO~~) Once the hrcoffice.com system was established, CLINTON's staff was provided email addresses on the new system. ABEDIN stated that [REDACTED] from PRN, assisted with setting up new accounts for CLINTON's staff. [REDACTED] also provided guidance on how to use the Microsoft Outlook based email system. ABEDIN did not know [REDACTED] or [REDACTED]

b6  
b7C

(U//~~FOUO~~) Prior to the transition to hrcoffice.com, ABEDIN was advised that the clintonemail.com system was "going away". ABEDIN stated that she lost most of her old emails as a result of the transition. She had only accessed clintonemail.com through a web portal and did not have a method for archiving her old emails prior to the transition. ABEDIN did not know if the system administrator had archived the mailboxes before the system was taken down.

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 8

(U//~~FOUO~~) ABEDIN remembered having discussions with HANLEY about creating an archive of CLINTON's emails. ABEDIN believed that the archive was placed on a laptop so that it could be referenced while CLINTON worked on her book. ABEDIN did not know that the laptop was sent to PRN, nor did she know what ultimately happened to the laptop. ABEDIN was not aware that a copy of the email archive may have been placed on a thumb drive.

### **Review and Production of ABEDIN Emails**

(U//~~FOUO~~) ABEDIN provided that she learned that DoS was seeking her emails after she read about it in the newspaper. DoS wanted ABEDIN's emails as part of an effort to ensure that DoS had a complete record of documents from CLINTON's tenure. ABEDIN contacted DoS and confirmed that it was seeking her emails. She noted that DoS' prior attempts to contact her were unsuccessful because DoS had an old email account and an old mailing address on file. ABEDIN then turned over her laptop and Blackberry to her attorneys so that they could conduct the review. ABEDIN was not directly involved in the review and relied on the judgment of her attorneys. RODRIGUEZ and DUNN stated that they sought additional guidance from DoS on how the review should be conducted but they never received a response. RODRIGUEZ and DUNN therefore erred on the side of caution and opted to include anything that they were unsure about. It was also noted that ABEDIN had previously responded to a similar request from the Benghazi Committee.

(U//~~FOUO~~) ABEDIN was shown an email chain dated April 2, 2012, with the subject "May - Asia". ABEDIN confirmed that the email was related to her activities while at DoS and that it would be considered a relevant record with respect to the DoS request. ABEDIN explained that this email was not produced by her team during the review because she did not have access to her clintonemail.com account when the review was conducted. RODRIGUEZ and DUNN stated that the request from DoS only sought records currently in ABEDIN's possession so they did not contact PRN to request other relevant records.

(U//~~FOUO~~) ABEDIN was not involved in the review and production of CLINTON's email, in response to a similar request that CLINTON received from DoS. ABEDIN stated that the review was conducted by CLINTON's attorneys and that she was not consulted during the process.

### **Private Residences**

(U//~~FOUO~~) CLINTON's residence in Washington, DC (Whitehaven) had a small office on the third floor that was converted to a SCIF by DoS. DoS removed the original door and replaced it with a metal door with a key code lock during the conversion. Inside the SCIF there was a desk where CLINTON worked and a computer, printer, facsimile machine and a television. DoS also installed a STE, a "yellow phone" and a video teleconference (VTC) system. ABEDIN provided that the door to the SCIF was not always locked and that ABEDIN, HANLEY and the [REDACTED] had access to the SCIF.

b6  
b7c



Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 9

(U//~~FOUO~~) CLINTON's residence in Chappaqua, NY, was also outfitted with a small SCIF that had the same equipment as the Whitehaven SCIF, less the television set. ABEDIN provided that CLINTON was the only person to use the SCIF and that she routinely used the Cisco telephone to make calls from Chappaqua because the cellular coverage was not very good there. ABEDIN, HANLEY and [REDACTED] all had access to the SCIF.

b6  
b7c

(U//~~FOUO~~) CLINTON received diplomatic pouches each night that contained the briefing material for the next day's meetings. When CLINTON was in Washington, she would be given the pouch prior to leaving DoS. If the pouch was not ready when she left, or if she was in New York, the pouch would be delivered to her residence by DS. The pouch would be received by the DS agent stationed at the house and would then be placed on a bench inside the residence. In Whitehaven, the bench was located outside of CLINTON's bedroom and in Chappaqua the bench was located near the main entrance. ABEDIN stated that it was less common for the diplomatic pouch to be delivered to Chappaqua because CLINTON would typically take the pouch with her when she was traveling. ABEDIN did not know if [REDACTED] ever received or transported the diplomatic pouch when it was delivered to the residence in Chappaqua. ABEDIN stated that [REDACTED] did not handle the diplomatic pouch at the Whitehaven residence because her shift ended before the pouch was delivered at 5PM.

b6  
b7c

(U//~~FOUO~~) CLINTON typically received the Presidential Daily Briefing (PDB) in person at the office. When she was not in the office the PDB would be delivered with the pouch or sent via secure facsimile. If the content was particularly sensitive she might be briefed in person by a CIA officer.

(U//~~FOUO~~) CLINTON would periodically receive both secure and unsecure facsimiles at her residence in Chappaqua. In order to receive a secure facsimile somebody would have to answer the phone and then wait several minutes for the documents to arrive. Since it was a time consuming process, [REDACTED] would sometimes assist CLINTON by answering or hanging up the facsimile system but he would leave the documents on the machine for CLINTON or her staff to collect. ABEDIN provided that [REDACTED] would pick up documents from the non-secure facsimile machine, which was located in a separate part of the residence. ABEDIN stated that they had numerous issues with the secure facsimile system in the Whitehaven residence and that it was often quicker to have the documents couriered to the house from DoS.

b6  
b7c

(U//~~FOUO~~) ABEDIN was shown an email chain dated March 20, 2009, with the subject "Re: Tomorrow". After reviewing the email ABEDIN stated that she knew for a fact that there were times when [REDACTED] assisted with the facsimile machine and may have collected documents from the secure facsimile machine for CLINTON. ABEDIN stated that the intention was to have CLINTON do it herself, but she wasn't very tech savvy and would get frustrated with the process. ABEDIN provided that the team would also occasionally email things to [REDACTED] or [REDACTED] to print for CLINTON.

b6  
b7c

### Miscellaneous

Continuation of FD-302 of Interview of Huma Abedin, On 4/5/2016, Page 10

(U//~~FOUO~~) ABEDIN provided that when CLINTON needed to contact the President she would have [ ] call the oval office to coordinate the meeting or call. ABEDIN believed that CLINTON had the President's email address but ABEDIN did not know what it was. ABEDIN noted that the President could only receive emails from approved addresses. She recounted that when CLINTON changed her primary email address they had to notify the White House so that CLINTON's emails would not be rejected by the server. ABEDIN was not sure how often CLINTON emailed the President. ABEDIN was shown an email chain dated June 28, 2012, with the subject "Re: Congratulations!" ABEDIN did not recognize the name of the sender. Once informed that the sender's name is believed to be a pseudonym used by the President, ABEDIN exclaimed "How is this not classified?" ABEDIN then expressed her amazement at the President's use of a pseudonym and asked if she could have a copy of the email. ABEDIN provided that she did not go on the trip to St. Petersburg and noted that security protocols in St. Petersburg were not necessarily the same as they were in Moscow, where they were not allowed use to their Blackberries.

b6  
b7c

(U//~~FOUO~~) ABEDIN was shown an email chain dated January 8, 2011, with the subject "Re: AG points from [ ]". After reviewing the email, ABEDIN provided that she vaguely recalled the email exchange and that the original email was sent in preparation for a call between the Attorney General and CLINTON. ABEDIN stated that she did not have concerns with the content because she was only a conveyor of the information and that she relied on the sender to properly mark any sensitive information. ABEDIN reiterated that she did not take it upon herself to question the sender's judgment on how a document should be marked. ABEDIN stated that people at DoS took the handling of classified information very seriously. She never had any concerns with how classified material was handled by individuals at DoS. Nor did she ever recall CLINTON expressing concerns over how classified information was handled.

b6  
b7c

(U//~~FOUO~~) ABEDIN first met SYDNEY BLUMENTHAL in 1996 when she was a junior staffer at the White House and BLUMENTHAL was a senior official. ABEDIN never worked directly with BLUMENTHAL but when CLINTON was in the Senate he would send emails for ABEDIN to pass to CLINTON. ABEDIN did not always forward the messages to CLINTON and BLUMENTHAL eventually stopped emailing ABEDIN when he realized this. When ABEDIN was at DoS, CLINTON would sometimes send ABEDIN emails from BLUMENTHAL for her to print. ABEDIN provided that she did not read the content of the emails from BLUMENTHAL and had no knowledge of his sources.

(U//~~FOUO~~) ABEDIN provided that she was not involved in drafting talking points while at DoS. The authors of the talking points depended on the content and were the responsibility of the appropriate bureau.

(U//~~FOUO~~) ABEDIN was shown an email chain dated September 20, 2012, with the subject "Re:". After reviewing the email ABEDIN stated that it was not common to stash the diplomatic pouch in the limousine but that it would have been secured by the DS or Secret Service (SS) agents that were with the car. ABEDIN noted that if they were in CLINTON's car there would be two DS agents present and if they took President CLINTON's car there would be one DS agent and one SS agent.

Continuation of FD-302 of Interview of Humna Abedin On 4/5/2016, Page 11

(U//~~FOUO~~) A copy of the original interview notes and the NDAs signed by RODRIGUEZ, DUNN and  are enclosed in a 1A envelope.

b6  
b7c

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/25/2015

(U//~~FOUO~~) On November 20, 2015 [redacted] date of birth [redacted] was interviewed at the [redacted] by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and [redacted]. After being advised of the identity of the interviewing agents, and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] joined the U.S. Department of State in [redacted] and has held the following positions:

b6  
b7C

- 
- 
- 
- 
- 
- 
- 
- 
- 
- 

b6  
b7C

(U//~~FOUO~~) [redacted] described the OpsCenter as the “eyes and ears” for the Secretary of State. The Ops Center is staffed 24 hours a day and constantly monitors reporting from Department of State cables, other government agencies and open source news outlets for information of interest to Department of State leadership. The Ops Center is also responsible for coordinating communications between senior leadership and foreign dignitaries. As a Senior Watch Officer (SWO) [redacted] was the most senior person in the Ops Center and was responsible for overseeing the activities of the other personnel as they worked to identify and disseminate critical information to the Secretary of State and Department of State leadership.

b6  
b7C

Investigation on 11/20/2015 at [redacted]

b6  
b7C

File # [redacted]-302 Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted]

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 11/20/2015, Page 2b6  
b7c

(U//~~FOUO~~) There are approximately seven or eight individuals staffed in the Ops Center during a normal day shift. In addition to the SWO, there are the following positions:

- Watch Officer (WO) – The WO is typically a junior civil servant who is responsible for gathering important information and disseminating it to Department of State leadership as necessary. They are responsible for answering incoming calls, monitoring cable traffic and scheduling phone calls for senior Department of State personnel as necessary.
- Emergency Action Officer (EAO) – The EAO is responsible for monitoring international hot spots and other current items of interest for the Department of State. They usually work with the Crisis Management Support team, which is collocated in the Ops Center.
- Ops Specialist – The Ops Specialist primarily performs clerical work for personnel in the Ops Center. This may include sending and receiving facsimiles or arranging the logistics of meetings or calls for Department of State leadership.
- Consular Affairs Officer – The Consular Affairs Officer is responsible for addressing any matters relevant to standard consular duties at foreign U.S. establishments.
- Diplomatic Security (DS) Officer – The DS Officer is a liaison between the Ops Center and the U.S. establishments and Regional Security Officers abroad.
- Swing Station – The swing station is an extra body that provides support to the SWO and the watch team as necessary.
- Bureau of Intelligence and Research (INR) Representative – The INR Rep is responsible for acting on behalf of the INR and for liaising with the broader Intelligence Community as necessary.

(U//~~FOUO~~) When urgent information or breaking news, which requires the immediate attention of senior Department of State personnel, is identified during normal working hours, the Director of the Ops Center is notified by the SWO. The Director communicates the information up the chain of command as appropriate. If such information is identified afterhours, the SWO notifies the Deputy Assistant Secretary (DAS) directly. The DAS will then provide the SWO with guidance on how the information should be transmitted.

(U//~~FOUO~~) During [REDACTED] tenure as a SWO there were two different Directors for the Ops Center. [REDACTED] was the Director for the majority of [REDACTED] time in the Ops Center, and upon [REDACTED] departure, [REDACTED] became the Director.

b6  
b7c

(U//~~FOUO~~) [REDACTED] did not recall ever emailing the Secretary directly and had no knowledge of the Secretary's personal email account or private email server. [REDACTED] only recalled receiving a few emails from the Secretary, such as mass emails at the holidays, which she

b6  
b7c

Continuation of FD-302 of Interview of [REDACTED], On 11/20/2015, Page 3b6  
b7C

presumed were sent from a Department of State email account. In instances where she needed to relay information to the Secretary she would send the information to the Secretary's Chief of Staff (CoS), or to HUMA ABEDIN.

(U//~~FOUO~~) [REDACTED] was shown a copy of the email that she sent on July 3, 2009, with the subject "Summary of 1055 EDT DPRK Conference Call", which was flagged by the ICIG as possibly containing classified information. [REDACTED] recalled the events surrounding the email and provided that she was the SWO on duty that day and had been directed to convene a call for key Department of State officials to discuss the DPRK missile launches. The discussion was based on afterhours reporting from the Intelligence Community that was at least confidential if not classified. [REDACTED] could not definitively recall what agency owned the source reporting but believed that it likely came from the Central Intelligence Agency. [REDACTED] was on the conference call for the purpose of taking notes but she was not an active participant in the discussion. [REDACTED] could not recall if the call was on a secure line but noted that it was common for such calls to be held on unclassified phone lines because not all of the key participants would have access to a secure phone if they were at home or traveling.

b6  
b7C

(U//~~FOUO~~) Following the call, [REDACTED] was responsible for summarizing the discussion in the referenced email and then forwarding it to individuals within the Department of State who needed to be aware of the situation. The email was sent on the unclassified system because not all of the intended recipients had immediate access to classified email accounts. [REDACTED] noted that it was not uncommon for the Ops Center to send such emails on the unclassified system. The specific content of the email was based on [REDACTED] notes and her judgment on what should be included in the summary. There was no formal review of the email, for either its content or for the presence of classified material, prior to it being sent. [REDACTED] noted that the Deputy Executive Secretary was an Original Classification Authority (OCA) who would on occasion review material for the Ops Center.

b6  
b7C

(U//~~FOUO~~) The email recipients were based on an established call sheet that indicated who should receive reporting on various topics. Also included were individuals added by the senior leadership. [REDACTED] identified the email recipients on the above cited email and provided the following information about their roles at that time:

b6  
b7C

- [REDACTED] was stationed in New York at the time. [REDACTED] could not recall her specific position but provided that she held a high ranking function within the United Nations.
- [REDACTED]
- [REDACTED]

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 11/20/2015, Page 4b6  
b7C

- [REDACTED]
- [REDACTED] could not recall her specific position or title.
- [REDACTED]
- [REDACTED] were staffers for other bureaus within the Department of State.

b6  
b7C

(U//~~FOUO~~) [REDACTED] reviewed the subsequent emails in the chain and noted that [REDACTED] was the SWO on duty on July 4<sup>th</sup>. Based on the time difference between when the conference call occurred and when the emails were sent, [REDACTED] believed that there may have been another SWO, or two, on duty between her shift and [REDACTED] shift. [REDACTED] could not recall who relieved her at the end of her shift but stated that she would have briefed the incoming SWO on the conference call and any necessary follow up items that the incoming SWO would need to address during their shift.

b6  
b7C

(U//~~FOUO~~) [REDACTED] provided that the Ops Center maintains a Watch Log where the details of any call arranged by the Ops Center are recorded. The log contains basic information about the call to include the date, time, participants, and in some cases a brief synopsis of the subject of the call. The Ops Center will log any calls that are facilitated by the Ops Center, which involve the Secretary of State, or any Deputy Secretaries, Under Secretaries, Assistant Secretaries, or foreign dignitaries. The Ops Center does not maintain a log for emails sent to, or from, the Ops Center.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was amenable to recontact if necessary.

b6  
b7C

(U//~~FOUO~~) Agent notes are included in an attached 1A.

UNCLASSIFIED//~~FOUO~~ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 08-19-2016 BY J37J85T94 NSICG

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/01/2016

(U//~~FOUO~~) On May 28, 2016, CHERYL MILLS, date of birth [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [REDACTED] and SA [REDACTED] at the law offices of Wilkinson Walsh + Eskovitz, 1900 M Street NW, Suite 800, Washington, DC. Present for the interview was SAMUELSON's counsel, Beth Wilkinson, Partner, Alexandra Walsh, Partner, and Hal Brewster, Associate. Also present was FBI Section Chief Peter Strzok, as well as David Laufman, [REDACTED] and [REDACTED] from the Department of Justice (DoJ) Counterintelligence and Export Control Section. After being advised of the identities of the interviewing agents and the purpose of the interview, MILLS provided the following information:

b6  
b7C

(U//~~FOUO~~) Immediately after completing her service at the United States Department of State (State) in 2013, MILLS became personal counsel for HILLARY CLINTON. HEATHER SAMUELSON joined MILLS' firm, located in Chevy Chase, MD, sometime in 2014.

**Transition to Platte River Networks Server**

(U//~~FOUO~~) When the respective offices of WILLIAM and HILLARY CLINTON began a search for a company to operate and maintain an email server, the CLINTON's financial manager recommended [REDACTED] as a technology broker. There were no security concerns with the CLINTON's then-current email server operated by BRYAN PAGLIANO (Pagliano server). The CLINTON's wanted an outsourced company accountable for the operation of the server. MILLS coordinated the needs for the server by providing non-technical guidance to [REDACTED] which was focused on the end user experience. After [REDACTED] identified several companies as options, the Office of President CLINTON reviewed the recommendations and selected Platte River Networks (PRN). After PRN was selected to procure, operate, and maintain the server (PRN server), MILLS negotiated the final cost and addressed privacy concerns with PRN. Throughout the negotiation process, MILLS consulted with PAGLIANO to ensure the recommendations of PRN would meet the end user experience guidance she had provided to PRN.

b6  
b7C

(U//~~FOUO~~) When PRN completed the transition from the Pagliano server, MILLS did not know if PRN transferred any email to the PRN Server. Additionally, MILLS did not know what PRN planned to do with the Pagliano server after the transition was complete.

Investigation on 5/28/2016 at Washington, DCFile # [REDACTED] 302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b3  
b7Eb6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UNCLASSIFIED//~~FOUO~~



Continuation of FD-302 of Interview of CHERYL MILLS, On 5/28/2016, Page 2**Department of State Request**

(U//~~FOUO~~) In the Summer of 2014, State was in the process of producing materials for the House Select Committee on Benghazi and raised concerns with MILLS regarding the lack of email for CLINTON. MILLS met with State personnel [redacted] and [redacted] who told MILLS State had no electronic records for CLINTON, other former Secretaries of State, and some other State personnel. MILLS understood the issue to be that State's computer systems taped over backup records after a period of time for all users not on the seventh floor and some users on the seventh floor. MILLS suggested to State they search State systems for CLINTON's clintonemail.com address, while State requested MILLS produce CLINTON's email. State provided no initial deadline in the first meeting and followed up with a letter documenting the request. MILLS understood State's request to be in relation to the Benghazi Committee and not a Freedom of Information Act (FOIA) request.

b6  
b7C

(U//~~FOUO~~) CLINTON asked MILLS and DAVID KENDALL to oversee the process of providing State CLINTON's emails from her tenure as Secretary of State. As the process was developed, [redacted] advised MILLS it was CLINTON or MILLS' obligation to filter out personal emails from what was provided to State. Additionally, if State received all CLINTON's emails involving .gov accounts, State would not filter out personal emails.

b6  
b7C**Collection of Relevant Email**

(U//~~FOUO~~) Late in the Summer of 2014, MILLS contacted [redacted] at PRN and requested all CLINTON's email involving a .gov account from her tenure as Secretary of State. MILLS believed [redacted] search for .gov email encompassed email headers, the body of emails, and any forwarded emails. She was not aware of which mailboxes or other potential locations [redacted] searched for email responsive to her request. However, MILLS did not believe [redacted] was asked to search or searched HUMA ABEDIN's clintonemail.com account. After preparing a .pst file of the .gov emails (July Export) based on MILLS' request, [redacted] discussed different options on the transfer of the July Export with MILLS, to include shipping DVDs, but [redacted] recommended a secure remote transfer. Based on [redacted] advice, MILLS neither requested nor received DVDs containing the July Export.

b6  
b7C

(U//~~FOUO~~) After deciding on the remote transfer, [redacted] provided MILLS with a link which provided [redacted] remote access to MILLS' computer. MILLS clicked on the initial link, then clicked an additional acknowledgement giving [redacted] permission to remotely access her computer. [redacted] then transferred the July Export to MILLS' computer and imported it into Outlook. Once the process was complete, MILLS revoked [redacted] permission and the remote session was terminated. MILLS did not know where [redacted] saved the .pst file on her computer or if it was encrypted, however, MILLS did recall the .pst file was password protected. Sometime after

b6  
b7C

Continuation of FD-302 of Interview of CHERYL MILLS, On 5/28/2016, Page 3

MILLS received the transfer, HEATHER SAMUELSON received a similar transfer from PRN. MILLS never made copies of the .pst file or transferred it to external media.

(U//~~FOUO~~) MILLS' Dell laptop (Dell) was the computer that received the transfer described above. The Dell was primarily used for work, but was sometimes used for personal reasons. It was connected to the Internet and had up-to-date antivirus software installed. The Dell was not wiped, other than PRN actions described later, or reset to a factory state. MILLS continued to use the Dell until it was turned over to her attorney BETH WILKINSON. The Dell is currently in WILKINSON's possession.

(U//~~FOUO~~) Shortly after SAMUELSON began reviewing the July Export from PRN, she noticed there was no email from approximately January 2009 – March 2009 in the data provided by PRN. MILLS likely reached out to [REDACTED] regarding this matter. [REDACTED] told MILLS PRN did not have any email for CLINTON from the timeframe in question. Since CLINTON was using AT&T for BlackBerry service during that time, MILLS recalled learning AT&T did not keep email records, but did not recall when she became aware of that fact. MILLS did not contact any other email service providers, such as Gmail, because she did not have knowledge of CLINTON using another email service. Additionally, MILLS did not recall attempting to access an Apple server that was once in operation at the CLINTON residence in Chappaqua, NY.

b6  
b7C

(U//~~FOUO~~) After reviewing a document dated July 28, 2014 referencing a conference call between MILLS, [REDACTED] and PAGLIANO regarding archived email options, MILLS stated she did not recall the specific conversation. Other than the conversation described above, MILLS did not recall any other conversations with [REDACTED] about the request for CLINTON's email involving .gov accounts.

b6  
b7C

(U//~~FOUO~~) After SAMUELSON began the review of the July Export, but before her review was complete, MILLS contacted [REDACTED] and requested a .pst file containing all of CLINTON's email from her tenure as Secretary to review it for non .gov work related email (September Export). MILLS did not instruct [REDACTED] to search ABEDIN's email and did not know which mailboxes or email addresses [REDACTED] searched to produce the .pst file responsive to her request. PRN remotely transferred the .pst file to SAMUELSON, however, MILLS did not recall if the .pst file was transferred to MILLS' Dell. Other than the July Export and, possibly, the September Export, MILLS did not receive any other .pst file transfers from PRN. However, SAMUELSON, as the one conducting the review, sometimes contacted [REDACTED] directly and received smaller transfers when she identified gaps in .pst files from [REDACTED]. MILLS never had direct access to CLINTON's mailbox on the PRN server.

b6  
b7C

### **Cull and Review of Email**

(U//~~FOUO~~) The review methodology employed by SAMUELSON was developed by SAMUELSON, MILLS and KENDALL, but was executed by SAMUELSON. They did not consider using any commercially available e-discovery tools for the review and did not consult any individuals

Continuation of FD-302 of Interview of CHERYL MILLS, On 5/28/2016, Page 4

who were not agents of Clinton during the review process. They also did not discuss how to handle potentially classified emails during the review because they had no reason to believe any classified material was contained in the emails. Additionally, no emails were identified as containing potentially classified or sensitive information, therefore, no emails were removed during the review process.

(U//~~FOUO~~) The review process called for all email from CLINTON's tenure to be filtered for .gov email addresses, relevant keywords, and the names of government officials. The review took SAMUELSON several months and occurred at MILLS' office in Chevy Chase, MD. SAMUELSON used her own computer for the review and, as questions arose, SAUMELSON would print any email in question and ask for guidance from MILLS. Emails that contained a mix of work-related and personal content were treated as work related. Once the review was complete, SAMUELSON printed the approximately 30,000 work-related emails identified in the review. The printed copies were then provided to State in December 2014. SAMUELSON produced an electronic copy of the work-related emails which was later provided to KENDALL at Williams and Connolly. MILLS was not aware of who produced the electronic copy provided to the FBI or what the file was named. Other than emails where SAMUELSON requested MILLS' guidance, MILLS did not review the emails identified by SAMUELSON as work-related.

(U//~~FOUO~~) MILLS was unsure if SAMUELSON encountered duplicate emails during her review. If she did, MILLS was not involved in any efforts to remove duplicates from the collection provided to State. Regarding ABEDIN's account on clintonemail.com, MILLS did not know why no email between ABEDIN's account and CLINTON's account was part of the production to State. There was no distinction between the treatment of email to or from ABEDIN's clintonemail.com account and ABEDIN's state.gov account.

(U//~~FOUO~~) After State began reviewing the emails printed by SAMUELSON, Stated advised MILLS when specific emails were determined to be classified and instructed her to delete the emails in her electronic copy, then empty her deleted items folder.

(U//~~FOUO~~) After reviewing an email dated November 24, 2014 referencing an "urgent call" with "CESC," MILLS stated she did not recall participating in a call with [REDACTED] MILLS also did not recall SAMUELSON having trouble with her connection to the .pst files in the same approximate timeframe.

b6  
b7c

(U//~~FOUO~~) MILLS recalled a discussion with PRN where PRN explained, because of the way Outlook functions, it displayed CLINTON's current email address instead of the email address CLINTON used at the time each email was transmitted. This issue was not resolved and no emails produced to State were altered.

#### **Deletion of Email**

Continuation of FD-302 of Interview of CHERYL MILLS, On 5/28/2016, Page 5

(U//~~FOUO~~) In late 2014 or early 2015, MILLS contacted [ ] and requested he remove all .pst files from her computer. She was unsure if she discussed with PAGLIANO the software proposed by [ ] to effect the deletion. In January 2015, [ ] sent MILLS a link and, in a process similar to the file transfer process described above, took control of her computer in a remote session. [ ] checked the computer for the requested files and removed them using software that permanently deleted the files. MILLS did not know if BleachBit was the software used by [ ]. After he completed the process, MILLS looked with [ ] to verify the files were deleted. MILLS did not discuss wiping or deletion software with anyone who was not an agent of CLINTON at the time, nor did anyone other than [ ] remove files from her computer.

b6  
b7C

(U//~~FOUO~~) In December 2014 or January 2015, CLINTON decided she did not want to retain email beyond a 30 or 60 day retention policy, to include access to any historical content. MILLS contacted [ ] and conveyed this change, but did not specifically instruct him to remove any .pst files or archived mailboxes.

b6  
b7C

(U//~~FOUO~~) In March 2015, after notifying PRN of obligations to preserve materials relevant to CLINTON's email, MILLS contacted PRN to determine if any backups of CLINTON's email existed and, if so, where those backups were located. After discussing the matter with PRN, she instructed PRN to visit the datacenter where the Pagliano server was housed and review it to confirm no records existed on the old system. PRN could not locate any backup data on the Pagliano server or any of the associated equipment, however, MILLS instructed PRN to maintain the equipment. MILLS was not aware of PRN deleting any data related to CLINTON's email in March 2015, nor did she request PRN delete any data, to include .pst files or Datto backup files. Furthermore, MILLS did not instruct PRN to delete any data using BleachBit on March 31, 2015.

(U//~~FOUO~~) MILLS had no knowledge regarding the following topics:

- At the time it was created, an email archive of CLINTON's email, including content from her tenure as Secretary of State, created by MONICA HANLEY.
- HANLEY providing the computer she created the archive on to [ ] in early 2014.
- [ ] returning the above computer containing the archive in 2014.
- Any transfer of clintonemail.com content to hrcoffice.com.
- CLINTON's access, or lack thereof, to her clintonemail.com content after CLINTON's hrcoffice.com email address was created.
- HUMA ABEDIN's method for accessing email.
- A master copy containing all of CLINTON's email from her tenure as Secretary of State.
- PRN email exports from September 2015.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes are enclosed in a 1A envelope.

~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

-I-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/13/2016

(U//~~FOUO~~) On April 9, 2016, CHERYL MILLS, was interviewed by Special Agent (SA) [redacted] and SA [redacted] inside the FBI Washington Field Office, 601 4<sup>th</sup> Street NW, Washington, DC 20535. Present for the interview were MILLS' attorneys Beth Wilkinson, Alexandra M. Walsh, and Hal Brewster from Wilkinson, Walsh & Eskovitz LLP. Also present was FBI Section Chief Peter P. Strzok, as well as David Laufman, [redacted] and [redacted] from the Department of Justice (DOJ). Prior to the interview, Wilkinson, Walsh, and Brewster agreed to sign a non-disclosure agreement in anticipation of viewing documents during the interview that were classified as part of a Special Access Program (SAP).

b6  
b7C

(U//~~FOUO~~) Prior to the interview, agents advised MILLS that while it was understood that the interview was being limited to the period of her Department of State (DoS) employment, the FBI believed it essential to the investigation to understand the sort process and the computers used in that process. Furthermore, MILLS was advised the FBI expected to continue the interview after the details were resolved by the attorneys. After being advised of the identities of the interviewing agents and the purpose of the interview, MILLS provided the following information:

(U//~~FOUO~~) From 1992 to 1999, MILLS served in the White House as Associate Counsel to the President. From 2002 to 2009, MILLS served as the Senior Vice President and General Counsel at New York University. MILLS also served as a consultant to HILLARY R. CLINTON's 2008 Presidential Campaign. In 2009, MILLS transitioned with CLINTON from the campaign to the Department of State (DoS). Initially, from January 2009 until May 2009, MILLS served in a part-time capacity as Acting Chief of Staff. She converted to full-time Chief of Staff and Counselor for Policy related to Food Security and Haiti thereafter. MILLS resigned from DoS in February 2013.

(U//~~FOUO~~) HUMA ABEDIN and JACOB SULLIVAN were also part of CLINTON's DoS executive staff. ABEDIN served as Deputy Chief of Staff for Operations and SULLIVAN served as Deputy Chief of Staff for Policy. [redacted] was also assigned to CLINTON's executive staff as [redacted] position was separate from that of the [redacted]

b6  
b7C

Investigation on 04/09/2016 at Washington, D.C.

File # [redacted] Date dictated N/A

By SA [redacted] SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~

NF

b1  
b3Continuation of FD-302 of Interview of Cheryl Mills, On 04/09/2016, Page 2

(U//~~FOUO~~) MILLS held a Top Secret/Sensitive Compartmented Information (SCI) clearance while at DoS. MILLS believed she likely had security training from Diplomatic Security (DS) upon receiving her clearance, but didn't recall any specific training. MILLS was not aware, nor was she ever told, she was a DoS original classification authority.

(U//~~FOUO~~) MILLS did not recall receiving any specific training or guidance concerning Federal Records retention policy or procedure during her DoS tenure, but explained it could have happened.

(U//~~FOUO~~) MILLS' unclassified DoS email account was MillsCID@state.gov. This account was linked to her DoS issued Blackberry and could also be accessed from her unclassified DoS computer or remotely via a fob system. MILLS further stated that the DoS fob system was not always reliable, and sometimes "went down." MILLS maintained a Gmail account, [REDACTED]@gmail.com, that she would use when she could not access her DoS unclassified account. Said Gmail account was the only personal account used by MILLS during her DoS tenure.

b6  
b7C

(U//~~FOUO~~) MILLS was able to switch over to a classified network in her DoS office. She was unsure as to what level of classification said network could handle, but knew that it could at least handle material declared as Secret.

(U//~~FOUO~~) When MILLS needed to review Top Secret materials, information was provided to her in person and taken away after she reviewed the materials. MILLS was not familiar with the JWICS system, and was not sure who may have had a JWICS account at DoS.

(U//~~FOUO~~) MILLS was asked to review an email dated 6/4/2011 and with the subject line "Google email hacking and woeful state of civilian technology." In response to the email, MILLS stated she did not recall the email, but the content was not unfamiliar to her. MILLS remembered hearing that hackers may have been targeting Gmail accounts, and further recalled somebody suggesting her account may have been targeted, but she was unsure of who provided her with this information. [REDACTED] the originator of said email, traveled a lot and had frequent difficulties signing into the DoS network, so it was common for her to use personal email.

b6  
b7C

(U//~~FOUO~~) Agents asked MILLS to review a DoS cable dated 6/28/2011 with the subject line "Securing Personal E-mail Accounts." MILLS did not recall the cable, but stated that it was probably connected to the 6/4/2011 email she previously reviewed. MILLS did not believe the referenced cable resulted in a "perfect" change of behavior in regards to the use of personal email accounts by DoS employees.

(U//~~FOUO~~) MILLS was asked to review an email dated 7/22/2011 with the subject line "Draft High-Level Narrative and Work Plan [Note Use of Personal/Gmail]." MILLS stated she "did not recall what she meant by (writing) 'Note Use of Personal/Gmail.'" in the subject line.

~~TOP SECRET~~

NF

b1  
b3

~~TOP SECRET~~b1  
b3Continuation of FD-302 of Interview of Cheryl Mills, On 04/09/2016, Page 3

(U//~~FOUO~~) The only mobile DoS device MILLS was issued was a Blackberry. Most, but not all, people at DoS were assigned a Blackberry. MILLS was not assigned a mobile secure phone, but she was able to check one out from the DoS communication team if/when needed.

(U//~~FOUO~~) MILLS did not travel with CLINTON as often as ABEDIN and/or SULLIVAN. MILLS only traveled with CLINTON on occasion when she visited Caribbean, African, or South American countries. When CLINTON traveled, MILLS ordinarily stayed back in Washington, DC, to manage DoS in her absence. MILLS recalled receiving travel briefings from DS prior to her DoS related travel.

(U//~~FOUO~~) MILLS was involved with the team that helped CLINTON transition to DoS. MILLS' role was to help CLINTON identify the priorities she wanted to address as Secretary. MILLS also identified individuals for CLINTON's staff. MILLS further saw her role as helping CLINTON "balance her life in regards to the transition." MILLS had no recollection of being involved with discussions concerning the structure of CLINTON's Information Technology (IT) platform during or after the transition.

(U//~~FOUO~~) Agents asked MILLS to review two emails from February 2009 with the subject lines "Update" and "Recap - Meeting re:Blackberries." While MILLS did not recall the specific emails, she stated she recalled the issue the emails referenced. MILLS explained CLINTON used a Blackberry to communicate prior to coming to DoS. CLINTON was not computer savvy and thus was not accustomed to using a computer, so efforts were made to try to figure out a system that would allow CLINTON to operate as she did before DoS. CLINTON did not have a computer in her DoS office. MILLS recalled hearing that the National Security Agency (NSA) had secure Blackberry technology that would allow for the use of such devices in a SCIF. MILLS requested DoS communication and security personnel research the possibility of implementing said technology at DoS. Ultimately it was decided that although the technology existed, it was not feasible to implement the same technology at DoS.

(U//~~FOUO~~) When asked what her understanding was in regards to who the six proposed secure Blackberry users were at DoS, as referenced in the email, MILLS explained that the goal was to obtain the technology for CLINTON because she did not have a computer. MILLS was not aware of who else at DoS may have received a secure Blackberry had the technology been approved for use at DoS.

(U//~~FOUO~~) The executive suite at DoS was termed "Mahogany Row," because of the wood paneling throughout the space. Mahogany Row was a SCIF, so the use of Blackberries was not authorized. MILLS was not familiar with waivers issued to previous Secretaries of State, which allowed for use of Blackberries in a DoS SCIF.

(U//~~FOUO~~) MILLS was asked to review a March 2009 DoS Memo with the subject line "Use of Blackberries in Mahogany Row." The memo, from ERIC J. BOSWELL, was addressed to MILLS. MILLS stated she "did not recall the memo, but it was not unfamiliar." MILLS believed the memo was in

~~TOP SECRET~~b1  
b3

~~TOP SECRET~~~~TOP SECRET~~b1  
b3

Continuation of FD-302 of Interview of Cheryl Mills, On 04/09/2016, Page 4  
response to inquiries and discussions held early on in CLINTON's DoS tenure concerning the possible use of Blackberries in sensitive DoS spaces. However, MILLS further explained that CLINTON and her executive staff did not use Blackberries on Mahogany Row because they were never authorized to do so.

(U//~~FOUO~~) When CLINTON wanted to email, she would have to leave Mahogany Row to retrieve and use her Blackberry. When CLINTON was inside of DoS Headquarters, most information was relayed to her face to face or on the phone. CLINTON also liked to receive and read a lot of information in paper documents, which is why she would often forward emails to her executive staff with instructions to print. MILLS was not aware of anyone other than CLINTON who had access to CLINTON's email account.

(U//~~FOUO~~) MILLS was not aware of CLINTON ever being issued a DoS Blackberry, nor could she recall any official request made for CLINTON to receive one. Agents asked MILLS to review an email dated 8/30/2011 with the subject line "Communications." After viewing the email, MILLS stated that she believed the exchange was in reference to conversations about communication issues during Hurricane Irene. MILLS recalled CLINTON's email was down during that time. Agents asked MILLS what was meant in the email by discussing the creation of a DoS email account that could "mask her identity, but which would also be subject to FOIA requests." MILLS explained she assumed "masking her identity" was in reference to the ability to give CLINTON a pseudonym so her account was not obvious to outside parties. MILLS also explained she thought that the FOIA reference meant that CLINTON's emails from the potential account would be subject to FOIA if the filing party knew the pseudonym.

(U//~~FOUO~~) Agents asked MILLS to review an email dated 1/24/2009 with the subject line "Series of Questions." MILLS stated she recalled the context of the email. As MILLS previously mentioned, CLINTON did not know how to use a computer, so the suggestion of a stand alone computer for CLINTON was not an appropriate solution.

(U//~~FOUO~~) CLINTON's office was connected to MILLS' office, so she would generally walk into CLINTON's office to share information MILLS received from relevant emails. MILLS wanted to create the best flow of information to the Secretary possible. MILLS stated she had no general concerns on how DoS business was handled on unclassified systems.

(U//~~FOUO~~) When CLINTON first came to DoS, she was using an email account associated with her AT&T Blackberry ([hr15@att.blackberry.net](mailto:hr15@att.blackberry.net)), and a few months later, CLINTON transitioned over to the [@clintonemail](mailto:@clintonemail) domain. MILLS did not know why CLINTON transitioned, but was aware of the transition because she was notified of the change in CLINTON's email address. MILLS further stated she was not aware of anyone at the time, from DoS or otherwise, who was responsible for the email transition.

(U//~~FOUO~~) It was MILLS' practice to use her State.gov email when conducting DoS business.

~~TOP SECRET~~~~TOP SECRET~~b1  
b3



~~TOP SECRET~~b1  
b3Continuation of FD-302 of Interview of Cheryl Mills, On 04/09/2016, Page 5

(U//~~FOUO~~) MILLS was not aware of any efforts to archive emails for federal records retention requirements or otherwise while she was at DoS. MILLS may have had conversations with BRYAN PAGLIANO concerning the Federal Records Act, but she was not sure. MILLS met with PAGLIANO frequently. MILLS did not recall any conversations with [REDACTED] concerning CLINTON's use of a private server and/or the Federal Records Act. MILLS stated that [REDACTED] name was familiar, but she did not recall any interactions she may have had with him.

b6  
b7C

(U//~~FOUO~~) MILLS recalled CLINTON using an iPad to review news articles. MILLS did not know if CLINTON used her iPad to email. MILLS was not aware of how many iPads CLINTON may have had during her DoS tenure. MILLS did not recall CLINTON using a "flip phone." MILLS was only aware of one mobile phone number for CLINTON.

(U//~~FOUO~~) MILLS did not recall any temporary email accounts or phone numbers being set up for CLINTON during Hurricane Sandy.

(U//~~FOUO~~) MILLS did not learn CLINTON was using a private server until after CLINTON's DoS tenure. MILLS stated she was not even sure she knew what a server was at the time. MILLS had no insight as to who came up with the idea of using the private server, nor was she aware of who made the final decision to use said server. However, MILLS believed the idea was to "piggyback" on the already existing server being utilized by President WILLIAM J. CLINTON. MILLS stated that there may have been technical people at DoS who were aware the Secretary was using a private server, but MILLS was only speculating. MILLS was not aware of any DoS procedures to approve the setup and use of a private server by CLINTON.

(U//~~FOUO~~) ABEDIN also had an account on the clintonemail.com domain. MILLS was not sure why she was not offered an account on the clintonemail.com domain, but stated that she was now "glad (she) did not have one."

(U//~~FOUO~~) MILLS was not familiar with the email address hr15@att.cingular.net. MILLS also stated she was "not aware of the email account [REDACTED]@gmail.com while at DoS."

b6  
b7C

(U//~~FOUO~~) It was MILLS' belief that the front office at DoS had a strong understanding of the need to maintain federal records. Agents asked MILLS to review an email dated 12/11/2012 with the subject "Significant FOIA Report." After reviewing the email, MILLS stated she was not sure if she was involved in the FOIA request filed by Citizens for Responsibility and Ethics in Washington (CREW) as discussed in the email. MILLS further explained there was a large volume of FOIA requests while she was at DoS. DoS Executives were made aware of significant FOIA requests, but it was not typical for MILLS to respond to FOIA because "it was not in her realm." MILLS also stated she "couldn't say who (at DoS) FOIA responses fell on."

~~TOP SECRET~~b1  
b3

~~TOP SECRET~~~~NT~~b1  
b3Continuation of FD-302 of Interview of Cheryl Mills, On 04/09/2016, Page 6

(U//~~FOUO~~) MILLS did not have knowledge of any backups or migrations of clintonemail.com accounts, nor was she aware of who might have knowledge of such events. MILLS was not aware of any emails being deleted or wiped from CLINTON's private email server prior to CLINTON leaving DoS.

(U//~~FOUO~~) Agents asked MILLS to review an email dated 10/13/2012 with the subject line "This am Green on Blue." After reviewing the email, MILLS stated she remembered the event, but not the specific email. MILLS did not know why [ ] might have forwarded her the email in question, but assumed it was "because he wanted her to read it." MILLS also noted the email was sent on a Saturday, so she was probably not in the office to receive the information directly from [ ]. MILLS further stated she did not have any concerns over the classification of the content of the email, nor that it was sent via an unclassified email.

b6  
b7C

(U//~~FOUO~~) Agents asked MILLS to review an email dated 2/20/2011 with the subject line "Follow Up to Davutoglu Call." After reviewing the email, MILLS stated she did not recall the email, nor could she speak as to [ ] reason for drafting the email and sending it to her. MILLS further explained if the media was interested in a story related to DoS, [ ] would have notified MILLS regardless of the sensitivity.

b6  
b7C

(U//~~FOUO~~) Agents asked MILLS to review an email dated 3/12/2011 with the subject line "radiation - fyi." After reviewing the email, MILLS stated she was not sure why [ ] would have sent her the email. [ ] was a private citizen [ ]. MILLS stated she could not recall what she meant when she typed "sending for info not for forwarding" before sharing [ ] email with CLINTON. MILLS had no concerns over her decision to forward the email on to [ ] STEPHEN MULL, or CLINTON.

b6  
b7C

[ ] MILLS recalled being read into Special Access Programs (SAP) during her DoS tenure, but did not recall the specifics concerning the SAPs or read-on process.

b1  
b3

(U//~~FOUO~~) MILLS was asked to review an email dated 12/23/2011 with the subject "(SBU)." After reading the email, MILLS stated the email originated from [ ] who was the [ ] and was forwarded to [ ] who was [ ] and later [ ]. MILLS stated she was "not surprised to see an email like this." She further stated that nothing in the email concerned her in regards to its classification. MILLS was not sure why [ ] would have sent the email string to MILLS' Gmail account rather than to MILLS' DoS account. MILLS

b6  
b7C~~TOP SECRET~~~~NT~~b1  
b3

~~TOP SECRET~~~~TOP SECRET~~b1  
b3Continuation of FD-302 of Interview of Cheryl Mills, On 04/09/2016, Page 7

further stated she did not recall if it was common to receive emails similar to the email in question in her Gmail account. MILLS was not aware of a formal process for providing notification of concurrence related to a High Value Target (HVT) to DoS Headquarters.

(U//~~FOUO~~) Agents asked MILLS to review an email dated 12/27/2011 with the subject "(SBU)." After reading the email, MILLS stated that she had no concerns regarding the classification of the email and her decision to forward CLINTON the email she received from [REDACTED] MILLS explained the goal was to observe what was going on in local media at the time, and she believed the email was related to that purpose.

b6  
b7C

[REDACTED] Agents asked MILLS to review an email dated [REDACTED] with the title [REDACTED] and another dated [REDACTED] with the title [REDACTED] The first of the two emails was sent on the DoS Secret network, whereas the latter of the two documents was sent via unclassified DoS email. Both emails pertained to [REDACTED] MILLS stated that she did not recall the originator of the document [REDACTED] nor did she remember the email, nor how the information contained in the email would have been relayed to CLINTON. At the prompting of her counsel, MILLS also stated she received between 400 and 700 emails a day while at DoS, and thus could not remember specific emails. MILLS stated she could not confirm if the information contained in the email agents asked her to review would have been relayed to CLINTON. [REDACTED]

b1  
b3

[REDACTED] MILLS did not have any concern over the content of the information in the email being sent on an unclassified system.

(U//~~FOUO~~) MILLS was involved in the development and draft process of some DoS policy memos, but it depended on the topic. Agents asked MILLS to review two of the same email dated 10/4/2009 with the subject "Draft Holbrooke Team" and an attachment titled "Pak Paper 10-03dcjjs.docx." One of the two emails was redacted by DoS in response to FOIA production, whereas the other was shown in a non-redacted format. MILLS stated she did not recall the information contained in the email she reviewed. MILLS did not know who would have drafted the memo. MILLS stated she was not familiar with the [REDACTED] Report."

b6  
b7C

(U//~~FOUO~~) According to MILLS, something might start in an unclassified format at DoS, but later be reclassified at a higher level when that information related to policy matters. MILLS was not sure who at DoS made the determination to change the classification.

(U//~~FOUO~~) MILLS did not recall any instances wherein she had concern over the way sensitive or classified information was handled at DoS. MILLS also did not recall any instances wherein CLINTON shared (with MILLS) any concerns over the way sensitive or classified information was handled at DoS.

(U//~~FOUO~~) A copy of the original interview notes is enclosed in a 1A envelope.

~~TOP SECRET~~~~TOP SECRET~~b1  
b3

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/2/2016

(U//~~FOUO~~) On February 1, 2016, STEPHEN D. MULL, DOB, [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] in his office at the United States Department of State (DoS), 320 21<sup>st</sup> Street NW, Washington, DC, Room 3417A. After being advised of the identities of the interviewing agents, and the purpose of the interview, MULL provided the following information:

b6  
b7c

(U//~~FOUO~~) MULL is a career DoS Foreign Service Officer. From 2009 until June of 2010, MULL served as a Senior Advisor to the Secretary of State on Political Affairs. In June 2010, MULL was appointed DoS Executive Secretary, a position in which he served until October 2012.

(U//~~FOUO~~) MULL later served as the United States Ambassador to Poland from November 2012 until September 2015. Thereafter, MULL was appointed to his current position, Coordinator for Iran Nuclear Implementation.

(U//~~FOUO~~) As Executive Secretary, MULL oversaw the entire DoS Executive Secretariat in regards to information processing, crisis management, travel support, and Information Technology (IT). MULL was more specifically tasked with overseeing the formal processing of information to and from the Secretary of State, HILLARY CLINTON, and her executive staff, to include the DoS Operations Center. This also included providing both mobile and in office IT support to the Secretariat.

(U//~~FOUO~~) While serving as Executive Secretary, MULL had very little direct interaction with the Secretary of State. MULL mostly interacted with the Secretary's Chief of Staff (COS) CHERYL MILLS.

(U//~~FOUO~~) Everybody in CLINTON's front office, except CLINTON herself, was on the Principal Officer Electronic Messaging System (POEMS) system. MULL communicated with CLINTON's executive staff via POEMS. MULL was not aware how messages sent to CLINTON's executive staff were relayed to CLINTON, but assumed they were orally briefed.

(U//~~FOUO~~) MULL was aware CLINTON was using a personal email account while at DoS. However, MULL had no role in setting up or maintaining CLINTON's personal account. MULL stated he did not know if the use of personal email accounts was common practice for previous Secretaries of State. MULL was not aware of a DOS policy at the time prohibiting the use of personal email accounts or servers. MULL further explained as Executive Secretary, he was responsible for overseeing the formal communications of the Executive Secretariat, but would not have been involved with providing and/or

---

Investigation on 2/1/2016 at Washington, D.C.File # [REDACTED] 302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b3  
b7Eb6  
b7C

Continuation of FD-302 of Interview of Steven Mull, On 2/1/2016, Page 2

maintaining information communication platforms. MULL did not know who assisted CLINTON in setting up the private email account and server she utilized at DoS. MULL did not know who was responsible for maintaining CLINTON's personal mobile communications devices, nor who was responsible for making sure the installation and use of said devices were within DoS policy.

(U//~~FOUO~~) Early into CLINTON's tenure as Secretary, MULL recalled being contacted by either MILLS or HUMA ABEDIN who asked about the possibility of the Secretary using an iPad to receive communications in her office. MULL recalled following up on their iPad inquiry, but explained he believed it was ultimately decided that CLINTON could not have the iPad in her office because of restrictions associated with her office being a Sensitive Compartment Information Facility (SCIF).

(U//~~FOUO~~) MULL never observed CLINTON using a mobile device in her office, but recalled seeing a picture of CLINTON using her Blackberry device on her DoS plane. MULL was unaware if there was any prohibition concerning the use of a Blackberry on the DoS plane.

(U//~~FOUO~~) MULL assumed Bluetooth capabilities were disabled on DoS issued mobile devices. MULL was not sure if CLINTON's private devices were configured the same way.

(U//~~FOUO~~) Agents asked MULL to review an email titled "S Communications," dated 8/30/2011, wherein it appears MILLS and ABEDIN ask MULL about the possibility of the Executive Secretariat issuing CLINTON a DoS Blackberry to use while her personal Blackberry was malfunctioning. MULL recalled informing ABEDIN and MILLS that while the Executive Secretariat could issue a DoS device, the DoS issued Blackberry would be subject to FOIA requests. MULL further recalled it was eventually decided CLINTON no longer needed the DoS device, and thus her request for a DoS Blackberry was never fulfilled.

(U//~~FOUO~~) MULL recalled receiving information from DoS Security [redacted] sometime in 2011, indicating there was concern over the possibility that some personal email accounts of DoS employees were hacked. MULL specifically recalled hearing CLINTON's Deputy Chief of Staff (COS) JACOB SULLIVAN's personal email account was amongst those compromised. [redacted] is currently assigned to the U.S. Embassy in [redacted]

b6  
b7C

(U//~~FOUO~~) MULL also provided the following names of individuals at DoS who had knowledge of CLINTON's IT setup during her tenure as Secretary of State:

(U//~~FOUO~~) [redacted] who worked under MULL was the [redacted] [redacted] for the Secretary and her executive staff.

b6  
b7C

(U//~~FOUO~~) TULINABO (TULI) MUSHINGI was the DoS Deputy Director for Administrative Support and supervised the DoS Mobile Communications Team. MUSHINGI is now the United States Ambassador to Burkina Faso.

Continuation of FD-302 of Interview of Steven Mull On 2/1/2016, Page 3

(U//~~FOUO~~) JOHN BENTEL managed the DoS POEMS system.

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/04/2015

(U//FOUO) [redacted] date of birth [redacted] was interviewed at his office at The [redacted]  
Washington, D.C. [redacted] mobile telephone number [redacted] by Federal Bureau of Investigation  
(FBI) Special Agents (SA) [redacted] and [redacted]. After being advised of the identity of  
the interviewing agents, and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] served as the [redacted] at the U.S.  
Department of State, under the former Secretary of State HILLARY CLINTON, from [redacted] until  
the end of CLINTON's term in February of 2013. [redacted] is a self described "Clintonista." His  
relationship with the CLINTONS dates back to [redacted]  
[redacted] under President Clinton. In 2009, [redacted]  
[redacted]

b6  
b7C

(U//FOUO) As the [redacted] held a TS/SCI clearance  
and was responsible for [redacted] any current  
Department of State matters. Each morning [redacted] worked with his staff to generate unclassified  
talking points and responses to [redacted]. This process often required the team  
to reference classified reporting to ensure that they had the proper context when formulating the response.  
The talking points were generated on the low side and were often based on reporting from the relevant  
country desk officer. Desk officers were responsible for coordinating information with external agencies  
as necessary, and were knowledgeable in how to protect sensitive sources and methods within their  
reporting.

b6  
b7C

(U//FOUO) Composing unclassified talking points required a continuous and conscious effort to  
evaluate if a given piece of information was derived from a classified or unclassified source. [redacted]  
described this process as an ongoing dilemma that they had to work through – How do you talk about  
diplomatic conversations in the public sphere without getting into details that may be confidential or  
protected? However, he noted that, they had grown up in this environment and knew how to separate  
classified information from unclassified statements. [redacted] provided that he and his team had  
received training on the handling of classified information.

b6  
b7CInvestigation on 11/03/2015 at Washington, D.C.File # [redacted]-302 Date dictated N/Ab3  
b7EBy SA [redacted] SA [redacted]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 11/03/2015, Page 2b6  
b7C

(U//FOUO) [REDACTED] worked very closely with CLINTON and would meet with her four or five times a day to ensure that [REDACTED] were consistent with the thoughts and statements of CLINTON. [REDACTED] initially traveled with CLINTON and then when she became comfortable with the position he stopped traveling to manage his team in Washington D.C. [REDACTED] would typically communicate with CLINTON via the Ops Center when she was traveling. [REDACTED] described CLINTON as a "paper person" noting that she preferred paper documents over electronic communications but he would email CLINTON when necessary. In these instances he would usually send the email to CHERYL MILLS who would either forward the message to CLINTON or respond on her behalf. On occasion he would email CLINTON directly. [REDACTED] did not receive any formal guidance on what, or when, to email CLINTON directly. This decision was based on his judgment.

b6  
b7C

(U//FOUO) [REDACTED] in the recent CLINTON email releases, many of which were related to the posting of diplomatic cables by Wikileaks in 2010. In April of 2010, [REDACTED] first began to get a sense of Wikileaks as it began to post Department of Defense information. Then in November of 2010 he was notified by [REDACTED] that the New York Times was preparing to publish a large number of diplomatic cables in conjunction with a Wikileaks release. Over the next several months [REDACTED] had regular contact with [REDACTED] as well as [REDACTED] to discuss cables that there about to be released. Upon receiving a media inquiry or a notification of an upcoming release, [REDACTED] would review the cable(s) in question and then make requests to the media outlet(s) to omit or redact specific information that was deemed sensitive for operational or diplomatic reasons. These requests were not always honored and [REDACTED] estimated that they had a .250 or .300 batting average. The Department of State had a rule by which they would not discuss any classified information in the cables but in instances where the cable was being incorrectly portrayed, or could easily be misconstrued by the reader, [REDACTED] would provide additional unclassified background information to set the proper context for the cable. [REDACTED] routinely worked with MILLS, and any agency that had an equity in the specific cable, to formulate the response to the media outlet.

b6  
b7C

(U//FOUO) Wikileaks, and other media leaks, posed a difficult problem for the Department of State because the information was already outside of the control of the Department of State and was often about to be published. While the Department of State could say nothing in response to a media notification or inquiry, the stance of the Department of State was to play defense and try to limit the potential damage by engaging the media outlet and providing a justification for why sensitive information should be omitted or redacted.

(U//FOUO) [REDACTED] first became aware of CLINTON's private email account when he received an email where "H" was the sender. He initially thought the email was spam but upon reading the message quickly realized that it was from CLINTON. Aside from the ambiguous username,

b6  
b7C



Continuation of FD-302 of Interview of [REDACTED]. On 11/03/2015. Page 3

b6  
b7C

[REDACTED] was not surprised that CLINTON was using a personal email account because it is a common practice within the Department of State. [REDACTED] had no knowledge about the setup of CLINTON's private server but assumed that Under Secretary PATRICK KENNEDY and MILLS would have been involved in that process.

b6  
b7C

(U//~~FOUO~~) [REDACTED] had no concerns about how CLINTON handled her communications during her tenure as Secretary of State. Nor did [REDACTED] have security concerns about anybody on CLINTON's team. He did not recall any instances where classified information was intentionally sent to, or from, CLINTON's email account. However, with respect to the emails on Benghazi, he noted that in hindsight some of the content should have been classified even though they did not believe it was classified at the time it was sent.

b6  
b7C

(U//~~FOUO~~) Due to the sensitivity of the matter, the interviewing agents verbally requested that [REDACTED] keep the interview and the nature of the discussion confidential. [REDACTED] verbally agreed that he would not discuss the interview with other parties.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was amenable to recontact regarding this matter, if necessary.

b6  
b7C

(U//~~FOUO~~) Agent notes are included in an attached 1A.

~~TOP SECRET~~ [redacted] ~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/21/2016

(U//FOUO) On March 15, 2016, [redacted] telephone number [redacted] [redacted] was interviewed by Special Agent (SA) [redacted] and SA [redacted] at the FBI Washington Field Office (WFO). After being advised of the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] served as the [redacted] [redacted] he was named [redacted] [redacted] [redacted] [redacted] remained [redacted] when he became [redacted] [redacted] retired from Department of State (DoS) in [redacted]

b6  
b7C

(U//FOUO) [redacted] did not get along with [redacted] and described him as a "big head." [redacted] further explained he thought [redacted] did not know his lane, specifically concerning his weekly updates to DoS Headquarters. [redacted] sent a weekly report directly to the Secretary of State when it was widely known "you didn't go direct" with the Secretary. Furthermore, there were concerns over [redacted] joining him on an unaccompanied post. [redacted]

b6  
b7C

(U//FOUO) [redacted] [redacted]

b6  
b7C

(U//FOUO) During his entire DoS tenure, [redacted] was never in direct contact with the Secretary of State. [redacted] was not aware HILLARY R. CLINTON was using a personal email address for DoS business, nor that she was operating off a private email server while she was Secretary of State. When [redacted] needed to relay a message that required the attention of the Secretary, he would follow the chain of command and go through an Assistant Secretary of State. [redacted] main DoS contact at that level was [redacted]

b6  
b7C

Investigation on 03/15/2016 at Washington DC  
FBI # [redacted] Date dictated N/A  
by SA [redacted] SA [redacted]

b3  
b7E

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~ [redacted] ~~TOP SECRET~~

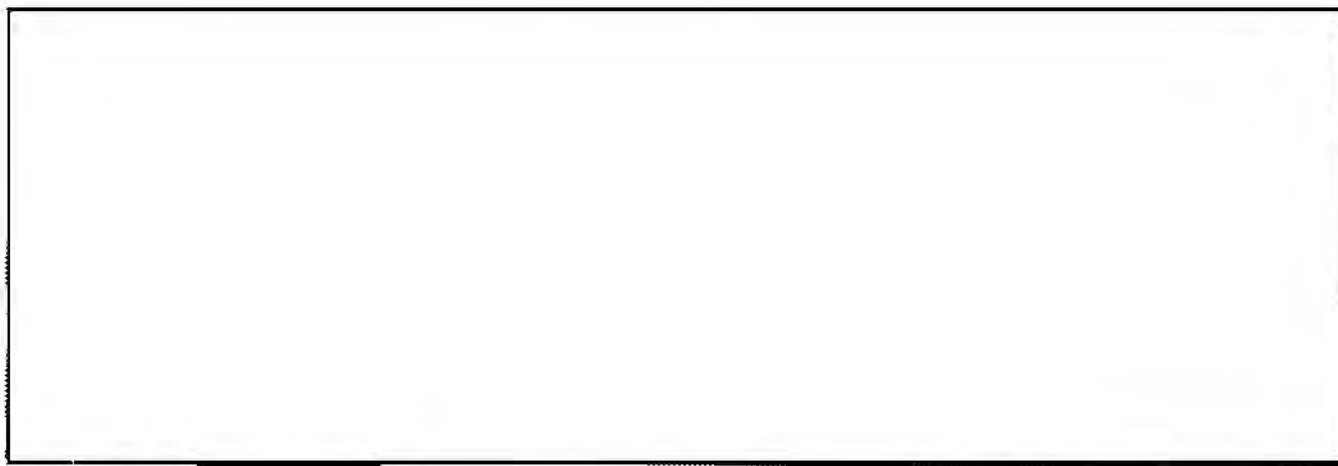
b1  
b3

~~TOP SECRET~~b1  
b3b6  
b7C

Continuation of FD-302 of Interview of [REDACTED] On 03/15/2010, Page 2  
 (U//FOUO) [REDACTED] understood any emails he sent to [REDACTED] or other contacts at DoS could be forwarded. He did not recall ever copying JACOB SULLIVAN, HUMA ABEDIN, or CHERYL MILLS, on emails because they were not in his chain of command. For urgent matters, [REDACTED] would follow protocol and contact the necessary parties via the DoS command center.

b6  
b7C

(U//FOUO) [REDACTED] recalled communicating directly with [REDACTED] prior to Secretary CLINTON's visit to Kazakhstan in 2010, but that was the only time he could recall going outside of his normal command channels.

b6  
b7Cb1  
b3

(U//FOUO) [REDACTED] had access to both DoS unclassified and secret networks at the Embassy in [REDACTED]. He could not recall if he had access to JWICS or a top secret network, but stated he did not use a top secret network.

b6  
b7C

[REDACTED] Agents asked [REDACTED] to review an email dated [REDACTED] with the subject [REDACTED]. After reviewing the email, [REDACTED] laughed and pointed out a portion in the email wherein he types, "My high side is down, so I'm summarizing this on this system." [REDACTED] explained it wasn't common for the high side to go down at the Embassy, but it sometimes happened. He further explained alternative options for communicating classified information would have been a secure call to the DoS Operations Center or "a carefully worded summary like this one" (a reference to the email he reviewed). [REDACTED] stated he found the email "fascinating" because it was just following the raid on the Usama Bin Laden (UBL) compound [REDACTED]. [REDACTED] further stated the email was "getting close to the line, obviously." However, he was not concerned about the email because it was just "business as usual" for he and others to have to communicate sensitive matters this way. [REDACTED] never received formal guidance on how to communicate information concerning [REDACTED] however, he stated that "if you are a professional, you know how to do it and how much to do."

b1  
b3~~TOP SECRET~~b1  
b3

~~TOP SECRET~~~~TOP SECRET~~b1  
b3b6  
b7C

Continuation of FD-302 of Interview of [REDACTED] On 03/15/2016, Page 3

[REDACTED] Agents asked [REDACTED] to review an email dated [REDACTED] with the subject [REDACTED]. After reviewing the email, [REDACTED] explained he did not recall the context of the email. [REDACTED] further explained that the people to whom the email was addressed were aware [REDACTED]. Furthermore, he had no concerns with sending the information contained in the email over an unclassified network because [REDACTED] believed he drafted the email so that it did not contain specific sensitive details.

b1  
b3

[REDACTED] Agents asked [REDACTED] to review an email dated [REDACTED] with the subject [REDACTED]. After reviewing the email, [REDACTED] explained he did not recall the context because there were [REDACTED]

b1  
b3

[REDACTED] Agents asked [REDACTED] to review an email dated [REDACTED] with the subject [REDACTED]. After reviewing the email, [REDACTED] exclaimed "again, this is right on the line." While [REDACTED] did not recall the specifics concerning the context of the email, he stated there were no details contained in the email that would compromise a sensitive program. [REDACTED] also pointed out that there were only three people involved in his original email.

b1  
b3

[REDACTED] Agents asked [REDACTED] to review an email dated [REDACTED] with the subject [REDACTED]. After reviewing the email, [REDACTED] stated that the email would have been sent around the time Pakistan closed off border crossings with Afghanistan, during which there was increased tension between Pakistan and the United States. [REDACTED] did not believe the information contained in the email was of concern [REDACTED]

b1  
b3

[REDACTED] Agents asked [REDACTED] to review an email dated [REDACTED] with the subject [REDACTED]. Agents noted that the email was sent on a classified network and marked SECRET//NOFORN. [REDACTED] stated that he sent the email on the Secret network because it was still during working hours in Washington, DC, compared to the previous emails he viewed that were sent after hours, and it made more sense for accessibility. The right method of sending a communication, according to [REDACTED] was whatever method allowed for the fastest possible dissemination of the message. According to [REDACTED] the SECRET//NOFORN marking and the sensitivity marking on the email he reviewed were automatically inserted as a default.

b1  
b3

[REDACTED] Agents asked [REDACTED] to review an email dated 7/6/2012 with the subject "US drone strike kills 4 militant in Pakistan." After reviewing the email, [REDACTED] stated "that's interesting." [REDACTED] RENDON (media/news service) was hired by DoS. [REDACTED] noted that [REDACTED] sent the news alert, and further complained that she was always "sticking her nose in where it didn't belong." [REDACTED] noted the information he added to the [REDACTED]

b1  
b3~~TOP SECRET~~~~TOP SECRET~~b1  
b3

~~TOP SECRET~~

[REDACTED]

~~NT~~

b1  
b3

Continuation of FD-302 of [REDACTED] Interview of [REDACTED]  
email chain

On 03/15/2016, Page 4

b6  
b7C

[REDACTED]

b1  
b3

(U//FOUO) A copy of the original interview notes is enclosed in a 1A envelope.

~~TOP SECRET~~

[REDACTED]

~~NT~~

b1  
b3

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/08/2016

b6  
b7C

(U//FOUO) On March 10, 2016, [REDACTED] former [REDACTED] [REDACTED] was interviewed by Special Agent (SA) [REDACTED] and SA [REDACTED] in an FBI office in New York, NY. After being advised of the identities of the interviewing agents and the purpose of the interview, [REDACTED] provided the following information:

(U//FOUO) [REDACTED] was the [REDACTED] Prior to his tenure [REDACTED] retired from Foreign Service. Following his retirement, [REDACTED] served as a visiting Professor [REDACTED] is currently [REDACTED] a non-government organization (NGO).

b6  
b7C

(U//FOUO) During his Department of State (DoS) tenure, [REDACTED] had very limited interaction with the Secretary of State. [REDACTED] assessed he likely only met Secretary HILLARY R. CLINTON in person on six occasions. These contacts occurred when [REDACTED] traveled back to Washington, DC, for various meetings, or when the Secretary visited [REDACTED] further assessed that during the same time period he only spoke with Secretary CLINTON via telephone on two to three occasions. [REDACTED] also participated in monthly Secure Video Teleconferences (SVTC) with the Secretary.

b6  
b7C

(U//FOUO) [REDACTED] was never in direct email contact with Secretary CLINTON and did not know Secretary CLINTON's email address. When [REDACTED] needed to relay a quick message back to DoS Headquarters, he would generally email direct with Deputy Secretary of State JACOB SULLIVAN or the Special Representative to Afghanistan and Pakistan (SRAP) office. [REDACTED] SRAP contacts included RICHARD HOLBROOKE, [REDACTED] and [REDACTED] also sent a regular Secret cable to Secretary CLINTON once a week. On rare occasions, [REDACTED] may have emailed the SRAP office or SULLIVAN via unclassified email to alert them to a classified cable. [REDACTED] was not sure how information he provided was briefed to Secretary CLINTON, but [REDACTED] "assumed the SRAP would brief at the level they saw fit."

b6  
b7C

Investigation on 03/10/2016 at New York, NY

b3  
b7E

File # [REDACTED] Date dictated N/A

By SA [REDACTED] SA [REDACTED]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~b1  
b3

Continuation of FD-302 of [REDACTED] Interview of [REDACTED] On 03/10/2016, Page [REDACTED]

b6  
b7C

(U//~~FOUO~~) There were three main ways [REDACTED] could report information back to DoS Headquarters:

b6  
b7C

1. Cable
2. Classified email usually for lateral information to other Ambassadors or to the National Security Council and [REDACTED]
3. Unclassified email for day to day interaction

b6  
b7C

(S//~~FOUO~~) [REDACTED] did not recall having access to IWICS or a Top Secret network [REDACTED]

b1  
b3  
b6  
b7C

[REDACTED] While he [REDACTED] was read into special access programs (SAPs) [REDACTED]

b1  
b3b1  
b3b1  
b3b1  
b3b1  
b3~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~b1  
b3

~~TOP SECRET~~ [REDACTED] ~~NT~~b1  
b3

Continuation of FD-302 of [REDACTED] Interview of [REDACTED] On 03/10/2016, Page 3

b6  
b7C

(U//~~FOUO~~) [REDACTED] was asked to review an email [REDACTED] with the subject line [REDACTED]. Upon reviewing the email, [REDACTED] commented "wow... I don't recall this email chain... I'm surprised to see it and prefer not to comment."

b6  
b7C

(U//~~FOUO~~) [REDACTED] was subsequently asked to review several other emails [REDACTED]. Upon reviewing each document, [REDACTED] again indicated he did not want to comment.

b6  
b7C

(U//~~FOUO~~) [REDACTED] stated that the reference to "talkers" in referenced document [REDACTED] related to "talking points" for foreign government discussions. [REDACTED] also explained the "SBU" caveat in the email meant "Sensitive but Unclassified" was a selected classification option in his unclassified email. Other classification options included "U" for unclassified, or "LU/SBU" Limited Use/Sensitive but Unclassified."

b6  
b7C

(U//~~FOUO~~) While being escorted to the elevator by SA [REDACTED] stated he recently read a news article about the investigation into Secretary CLINTON's personal email server that opined that most of the classified documents were over classified. However, [REDACTED] stated that after seeing the above referenced documents, he now understood why people were concerned about this matter.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes is enclosed in a 1A envelope.

~~TOP SECRET~~ [REDACTED] ~~NT~~b1  
b3



~~TOP SECRET//~~ [redacted] ~~NI~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/27/2016

(U//FOUO) On April 25, 2016, [redacted] former [redacted]  
[redacted] was interviewed by Special Agent (SA) [redacted] and SA [redacted] in the FBI  
Washington Field Office (WFO), 601 4<sup>th</sup> Street NW, Washington, DC 20535. Also present for the  
interview was [redacted] counsel, [redacted] as well as [redacted] and [redacted] from  
the Department of Justice (DOJ). The interview was conducted as a follow up to an interview of  
[redacted] conducted by SA [redacted] and SA [redacted] on March 10, 2016. Prior to the interview, [redacted]  
agreed to sign a non-disclosure agreement in anticipation of viewing documents during the interview that  
were classified as part of a Special Access Program (SAP). After being advised of the identities of the  
interviewing agents and the purpose of the interview, [redacted] provided the following information

b6  
b7C

[redacted]

b1  
b3

[redacted]

b1  
b3

[redacted]

b1  
b3

Investigation on 03/10/2016 at Washington, DC

File # [redacted] Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it  
and its contents are not to be distributed outside your agency.

~~TOP SECRET//~~ [redacted] ~~NI~~

b1  
b3

~~TOP SECRET~~~~TOP SECRET~~b1  
b3

Continuation of FD-302 of Interview of [REDACTED], On 04/25/2016, Page 2

b6  
b7Cb1  
b3b1  
b3b1  
b3b1  
b3b1  
b3b1  
b3

~~TOP SECRET~~b1  
b3

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 04/25/2016, Page 3

b6  
b7C

\_\_\_\_\_ usually communicated with Special Representative to Afghanistan and Pakistan (SRAP), \_\_\_\_\_, and \_\_\_\_\_ but assumed he must have also wanted to SULLIVAN to know, as he noted SULLIVAN was one of the recipients. \_\_\_\_\_ assumed SULLIVAN would relay information \_\_\_\_\_ to "anyone at DoS who needed to know," the Secretary of State, Deputy Secretary of States, etc. SULLIVAN was not given guidance on how to relay such information back to DoS Headquarters, but stated the email in question was sent at a time wherein it was important to report. \_\_\_\_\_ was not sure why he chose to send the email in question on a classified network.

b1  
b3

\_\_\_\_\_ Agents asked \_\_\_\_\_ to review an email dated 12/27/2011 with the subject "(SBU)." After reviewing the email, \_\_\_\_\_ explained he did not recall the context. However, \_\_\_\_\_ stated that the previously explained "cross border event" took place at the end of November 2011, so the email in question was sent shortly thereafter \_\_\_\_\_

b1  
b3

\_\_\_\_\_ Agents asked \_\_\_\_\_ to review an email dated 7/6/2012, with the subject "US drone strike kills 4 militants in Pakistan." After reviewing the email, \_\_\_\_\_ explained the email was sent \_\_\_\_\_. The email originated from an AP article found and forwarded to \_\_\_\_\_ subsequently forwarded the article to the Deputy Chief of Mission, \_\_\_\_\_

b1  
b3

\_\_\_\_\_ also stated that at the time he sent the email, he did not think the information he provided jeopardized anyone involved. \_\_\_\_\_ who was Cc'd on an email in the exchange was the \_\_\_\_\_ for the U.S. in Pakistan.

(U//FOUO) A copy of the original interview notes is enclosed in a 1A envelope.

~~TOP SECRET~~b1  
b3

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/11/2015

(U//~~FOUO~~) On December 11, 2015, [REDACTED]  
[REDACTED] U.S. Department of State, was interviewed by Federal Bureau  
of Investigation (FBI) Special Agents [REDACTED] and [REDACTED]. After being advised  
of the identities of the interviewing agents, and the purpose of the interview, [REDACTED] provided the  
following information:

b6  
b7C

(U//~~FOUO~~) [REDACTED] for the U.S. Department of State, from [REDACTED]  
[REDACTED] where she was responsible for [REDACTED]  
[REDACTED]. She assumed the role when [REDACTED] left the position. On a typical day  
[REDACTED] would meet with the then Secretary of State HILLARY CLINTON at the daily 8:30 A.M.  
meeting to discuss key issues [REDACTED]. During the meeting CLINTON  
would provide guidance on what should be communicated [REDACTED]. Prior to finalizing  
the briefing materials [REDACTED] would then work with the relevant Department of State components to  
verify the message and to add any necessary details. [REDACTED] did not deal with the U.S. Intelligence  
Community (USIC) aside from a daily interagency [REDACTED]  
[REDACTED] traveled with  
CLINTON on all of her foreign trips, during which [REDACTED] were handled by one of  
[REDACTED] deputies.

b6  
b7C

(U//~~FOUO~~) [REDACTED] stated that she saw CLINTON frequently throughout the day and as a  
result most of her communications with CLINTON were spoken. [REDACTED] could only recall one time  
when CLINTON emailed her directly and that was on the night of the Benghazi attack. [REDACTED] stated  
that at that time she had no knowledge that CLINTON was using a private email server. [REDACTED] noted  
that CLINTON was not an email person and therefore assumed that CLINTON was conducting personal  
business when she was on her Blackberry.

b6  
b7C

(U//~~FOUO~~) [REDACTED] also worked closely with JAKE SULLIVAN, CLINTON's Chief of Staff  
for Political Affairs, for routine matters. [REDACTED] understood that SULLIVAN would relay pertinent  
information to CLINTON but she did not know if SULLIVAN directly forwarded her emails to  
CLINTON or not. [REDACTED] provided that she occasionally interacted with CHERYL MILLS but did  
not have regular contact with HUMA ABEDIN.

b6  
b7CInvestigation on 12/11/2015 at Washington, D.C.File # [REDACTED] 302 Date dictated N/Ab3  
b7EBy SA [REDACTED] SA [REDACTED]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 12/11/2015, Page 2b6  
b7C

(U//FOUO) [REDACTED] reviewed an email, [REDACTED] that she sent on [REDACTED] with the subject [REDACTED] piece." She confirmed that she remembered the events surrounding the email. After carefully reviewing the entire email string [REDACTED] gave a brief overview of the Benghazi attack and provided that this email was sent after she learned that the New York Times was planning to publish an article about the Benghazi attack and the annex. The topic was of particular interest because at that time the media only knew of the Consulate in Benghazi and information on the annex had not yet been publicly released.

b6  
b7C

(U//FOUO) [REDACTED] further explained that [REDACTED] [REDACTED] was to notify Department of State leadership when the media was preparing to release information on sensitive or controversial topics. Alerting leadership allowed the Department of State an opportunity to engage the media outlet to negotiate what details should be released and to prepare an appropriate public response. [REDACTED] stated that she sent the email in question to alert Department of State leadership and National Security Council personnel of the upcoming article because of potential sensitivities around disclosing the existence of the annex. The subsequent messages in the email chain are responses from other individuals as they discussed a subsequent call that occurred with the New York Times that afternoon.

b6  
b7C

(U//FOUO) During the discussion [REDACTED] provided that she is participating in the Freedom of Information Act (FOIA) review process for the ongoing release of CLINTON's emails. [REDACTED] [REDACTED] has a team of individuals who are reviewing all emails pertinent to [REDACTED] prior to their release, to assess if they contain information that is either classified or represents an internal Department of State deliberation.

b6  
b7C

(U//FOUO) [REDACTED] explained that internal deliberations are internal discussions about various international affairs and policies. These conversations do not necessarily reflect the official, or final, stance of the Department of State on a specific topic. Additionally, the information may be misconstrued by the casual reader or cause embarrassment to the Department of State if it is released in its original form. When her team finds an email containing a deliberative discussion they mark the relevant sections for redaction under the B5 exception. [REDACTED] reviews the team's work before it is passed to the next phase of the review process within the Department of State. [REDACTED] noted that a significant number of the items that her group recommended for redaction because they were deliberative products were ultimately marked for redaction, by internal counsel, using the classified material (B1) exception. [REDACTED] did not know why internal counsel elected not to follow her group's recommendations but noted that as a result a significant number of FOIA released documents that are marked as containing classified information really only contain deliberative material.

b6  
b7C

(U//FOUO) [REDACTED] acknowledged that some of the emails marked as containing classified information did in fact have classified material. However, she quickly noted that she did not recall seeing anything that would potentially compromise national security or be considered criminal in nature.

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED]. On 12/11/2015. Page 3

(U//~~FOUO~~) [REDACTED] explained that the U.S. Department of State personnel commonly operate on the unclassified system. She gave the example of a diplomat who summarizes a diplomatic conversation on the unclassified computer system. In general, they don't believe such diplomatic conversations are classified because it is usually obtained through diplomatic discussions and not from sensitive sources. They would consider the discussion to be Sensitive But Unclassified (SBU) and transmitted on OpenNet with the expectation that it would be contained on the Department of State system and only accessed by legitimate users.

(U//~~FOUO~~) [REDACTED] was aware of the counterintelligence threats facing the Department of State and noted [REDACTED]

[REDACTED] Based on these experiences she is careful not to transmit sensitive information on the unclassified or unsecured systems and she advised her subordinates to do the same. However, despite her security posture she did not find fault with her colleagues who did otherwise.

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

b6  
b7C  
b6  
b7C

b6  
b7C

~~SECRET~~ // NOFORN

FD-302a (Rev. 10-6-95)

-1-

FBI INFO.  
CLASSIFIED BY: NSICG C28W34B64  
REASON: 1.4 (C)  
DECLASSIFY ON: 12-31-2041  
DATE: 09-22-2016

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/19/2016

(U//~~FOUO~~) On January 7, 2016, SIDNEY BLUMENTHAL was interviewed at the law offices of [redacted] NW, Washington, DC 20005 by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted]. Also present for the interview was BLUMENTHAL's attorney, [redacted] office telephone [redacted] email address [redacted] as well as Department of Justice attorneys [redacted] and [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, BLUMENTHAL provided the following:

b6  
b7C

(U//~~FOUO~~) BLUMENTHAL is a friend of HILLARY CLINTON (CLINTON). During her tenure as Secretary of State from 2009-2013, he served as an informal political advisor by sending emails containing information he deemed to be helpful and interesting topics. BLUMENTHAL did not recall sending any such emails prior to CLINTON becoming Secretary of State. There was no set schedule for these emails, BLUMENTHAL was never paid for his advisory services, and there was no specific conversation with CLINTON regarding his informal role. However, CLINTON would occasionally acknowledge the value of his emails in a response to BLUMENTHAL. During this time, BLUMENTHAL was also employed by the Clinton Foundation where his duties were related to former President BILL CLINTON, his legacy, and some communications of the Foundation. BLUMENTHAL reported to [redacted] and does not recall what HILLARY CLINTON's role was in defining his role at the Foundation. During this timeframe, BLUMENTHAL was also involved with the Clinton Global Initiative.

b6  
b7C

(S//~~FOUO~~) TYLER DRUMHELLER was a career Central Intelligence Agency (CIA) employee who served in a number of capacities during his tenure. [redacted]

b1

[redacted] During the timeframe in which BLUMENTHAL used DRUMHELLER as a source for information provided to CLINTON, DRUMHELLER was retired from the CIA. DRUMHELLER knew the information he provided would be forwarded to CLINTON and provided it because he thought the information would be useful and helpful to the United States Government (USG). He did not receive any compensation for the information. The caveats provided regarding the source of the information were directly from DRUMHELLER, with the

Investigation on 1/7/2016 at Washington, DC

File # [redacted] 302 Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Classified By: F36M72K12

Derived From: FBI TASC dated 20140702

Declassify On: 20411231

~~SECRET~~ // NOFORN

Continuation of FD-302 of Interview of SIDNEY BLUMENTHAL, On 1/7/2016, Page 2

exception of the CONFIDENTIAL marking BLUMENTHAL would frequently place at the top of his communications with CLINTON. The CONFIDENTIAL marking was meant to imply the email was of a personal nature from BLUMENTHAL and did not refer to classified USG information.

(U//~~FOUO~~) DRUMHELLER had a business with large corporate contracts, but BLUMENTHAL did not know specifically who these contracts were with or what they were for. During a conversation with DRUMHELLER regarding humanitarian aid projects, BLUMENTHAL conceived of a project that would provide field hospitals and aid to Libyan refugees. DRUMHELLER stated BLUMENTHAL would receive a finder's fee if the project materialized, but it did not come to fruition. This potential finder's fee was the only financial relationship between DRUMHELLER and BLUMENTHAL.

(U//~~FOUO~~) [ ] has been a friend of BLUMENTHAL for several years and was retired during the time when BLUMENTHAL used him as a source. BLUMENTHAL does not know where [ ] would get the information he provided. b6 b7C

(U//~~FOUO~~) [ ] is a journalist involved in international education and has been a friend of BLUMENTHAL's for decades. b6 b7C

(U) ~~(S//NF)~~ GARY BERNTSEN is a retired CIA officer who BLUMENTHAL met through LARRY JOHNSON, another former CIA officer. JOHNSON wanted BLUMENTHAL to hear BERNTSEN's story as described in BERNTSEN's book JAWBREAKER. Neither BERNTSEN nor JOHNSON ever stated they were providing classified information or that they obtained any information from the CIA. BLUMENTHAL did not ask if the information was classified.

(U//~~FOUO~~) [ ] is a former [ ] who BLUMENTHAL met when [ ] was assigned to [ ] in the 1980s. b6 b7C

(U) ~~(S//NF)~~ BILL MURRAY is a former CIA Chief of Station and a friend of DRUMHELLER.

(U//~~FOUO~~) [ ] was the [ ] during the GORDON BROWN and TONY BLAIR administrations. He is an old friend of BLUMENTHAL's and provided information on British politics and personalities. b6 b7C

(U//~~FOUO~~) [ ] was a [ ] who BLUMENTHAL met through [ ] BASHAR AL-ASSAD, as well as others in the [ ] government personally. He provided BLUMENTHAL with information on the ASSAD regime. b6 b7C

(U//~~FOUO~~) [ ] is an [ ] with experience in [ ] [ ] provided information he picked up and sometimes knew the information would be provided to CLINTON. b6 b7C



FD-302a (Rev. 10-6-95)

Continuation of FD-302 of Interview of SIDNEY BLUMENTHAL, On 1/7/2016 Page 3

(U//~~FOUO~~) BLUMENTHAL had no concerns regarding the sensitivity of the information he provided to CLINTON during her term as Secretary of State. Additionally, he does not believe any of it was classified.

(U//~~FOUO~~) BLUMENTHAL held a clearance in the 1997-2001 timeframe when he was an assistant to President BILL CLINTON. He recalled a quick briefing on security and clearances, but has no recollection of being read-on to any special programs.

~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/19/2016

b1 per CIA

b3

b6

b7C

b3 per CIA

(S//NF) On May 17, 2016 [redacted] was interviewed by Special Agent (SA) [redacted] and SA [redacted] at the Central Intelligence Agency (CIA) in McLean, Virginia. Also present for the interview was [redacted] CIA attorney [redacted]. After being advised of the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information:

b1 per CIA

b3

b1 per CIA

b3

b1 per CIA

b3

b1 per CIA

b3

Investigation on 05/17/2016 at McLean, VA

File # [redacted] Date dictated N/A

By SA [redacted] SA [redacted]

b3

b7E

b6

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~

b1

b3

~~TOP SECRET~~b1  
b3

Continuation of FD-302 of \_\_\_\_\_ Interview \_\_\_\_\_ On 05/17/2016, Page 2

b1 per CIA  
b3b1 per CIA  
b3b1 per CIA  
b3

\_\_\_\_\_ was shown a copy of an email from \_\_\_\_\_  
with the subject \_\_\_\_\_. After reviewing the email he provided \_\_\_\_\_  
that he would have classified the email if he was sending the information.

b1 per CIA  
b3

\_\_\_\_\_ was shown a copy of an email from \_\_\_\_\_  
with the subject \_\_\_\_\_. After reviewing the email, \_\_\_\_\_  
believed that the email was discussing \_\_\_\_\_ but stated that a casual reader would have a difficult  
time figuring out what the email was about.

b1 per CIA  
b3

\_\_\_\_\_ was shown a copy of an email from \_\_\_\_\_ with  
the subject \_\_\_\_\_. After  
reviewing the email \_\_\_\_\_ stated that he would not have put this information on an unclassified system  
but that the authors were only responding to a media article.

b1 per CIA  
b3

(U//FOUO) A copy of the original interview notes and the referenced documents is enclosed in a  
1A envelope.

~~TOP SECRET~~b1  
b3

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/2/2016

(U//FOUO) On December 31, 2015, [ ] of [ ] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [ ] and [ ]. Also present were Beth Wilkinson, Partner, and [ ] Attorney at Law, at Paul, Weiss, Rifkind, Wharton & Garrison LLP, 2001 K Street, NW, Washington, D.C., 20006, and [ ] U.S. Department of Justice. After being advised of the identities of the interviewing agents, and the purpose of the interview, [ ] provided the following information:

b6  
b7C

(U//FOUO) [ ] has worked for HILLARY CLINTON since [ ] when he was hired as her [ ]. In this role he served as [ ] worked on her campaign and was subsequently named [ ] when CLINTON became the Secretary of State (Secretary), at the U.S. Department of State (State). [ ] currently works at [ ] but noted that he still acts as a part time advisor to CLINTON.

b6  
b7C

(U//FOUO) [ ] reported to [ ] and was primarily responsible for leading the [ ] team and for acting as the Secretary's [ ]. [ ] traveled with the Secretary on all of her trips, with the exception of two or three trips. [ ] noted that zero percent of his official job function was related to Information Technology (IT) or the maintenance of the Secretary's phones or computers. However, [ ] was technically savvy and was frequently in contact with the Secretary and as a result she often asked him for assistance with such matters. [ ] likened it to your parents asking for technical help with their phone or computer.

b6  
b7C

(U//FOUO) [ ] had regular and ongoing contact with the Secretary and, as such, the majority of their communications occurred in person. However, he would communicate with her via phone or email when necessary. [ ] stated that he received his first email from CLINTON in 2007 and confirmed that she used the following email accounts: h15@att.blackberry.net, hdr22@clintonemail.com, [ ]@gmail.com during her tenure.

b6  
b7C

(U//FOUO) [ ] stated that he had no knowledge of CLINTON's private email server until it recently became public knowledge. [ ] knew JUSTIN COOPER because Cooper was a long time aide for Bill Clinton. [ ] never discussed the private server with COOPER until after it was

b6  
b7C

Investigation on 12/31/2015 at Washington, D.C.

b3  
b7E

File # [ ]-302 Date dictated N/A

By SA [ ] SA [ ]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7CContinuation of FD-302 of Interview of [REDACTED], On 12/31/2015, Page 2

documented in the press. Similarly, [REDACTED] knew BRYAN PAGLIANO but never discussed the email setup or any other IT matters with him.

b6  
b7C

(U//~~FOUO~~) Upon starting at State in 2009 [REDACTED] received a security clearance and received training on the handling of classified information. He was provided with a classified terminal at his desk but didn't have a reason to communicate classified information via email given his position. He could not recall any specific instances of using the classified email system and stated that he never transmitted anything marked as classified on an unclassified system.

b6  
b7C

(U//~~FOUO~~) [REDACTED] did not recall receiving any guidance from State on records management or the use of private email for official business. However, he noted that it may have been included in one of the numerous documents that he was required to sign when he first started at State. Nonetheless, he tried to use his official email for official business and his personal email for personal business. [REDACTED] noted that there were some instances where he would email the Secretary from his personal email account such as when he was at home or traveling and wanted to send an article or press clipping of interest to the Secretary. Other examples of when he did this included when he first started and did not have a government email account; times when there were system outages; or when he had difficulty remotely accessing the system. [REDACTED] provided that the Secretary neither approved of, or discouraged, the use of his private email account in these instances. [REDACTED] had no knowledge of any intrusions or attacks against either his personal or government email accounts.

b6  
b7C

(U//~~FOUO~~) [REDACTED] listed the Secretary as 'EVERGREEN' in his personal email contact list. He explained that this had been the codename used by the Secret Service since she was the first lady.

b6  
b7C

(U//~~FOUO~~) During the interview [REDACTED] was shown several emails that he had authored during his tenure at State while providing technical support to the Secretary. [REDACTED] reviewed each email and provided the following context:

b6  
b7C

1. The first email was sent in approximately 2010 after he purchased the first iPad for the Secretary. [REDACTED] did not recall the specifications for the device but believed it was the latest model available at that time. [REDACTED] purchased the iPad and configured it to use the [REDACTED]@gmail.com email account so that he could send articles of interest to the Secretary. [REDACTED] stated that she could not view the articles on her Blackberry and the iPad and email account were setup as a way to test a different delivery method. [REDACTED] did not recall the email account being used thereafter and was "fairly sure it wasn't used" after the initial setup.
2. The second email was sent just prior to the end of the Secretary's term but [REDACTED] could not recall any further details about the context of the email. [REDACTED] stated that he only

b6  
b7Cb6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 12/31/2015, Page 3

b6  
b7C

purchased one iPad for the Secretary and could not remember a second iPad, or any details of a recovery email account. [REDACTED] recounted how after he gave the Secretary the iPad, the Secretary fell asleep holding the unopened packaging in her arms. This struck [REDACTED] as funny because, in contrast, he would not be able to sleep if he had just received a new iPad. He noted that this episode was foreshadowing for how little she would use the iPad.

b6  
b7C

3. The third email referred to the cover of a People Magazine edition from August 2010 and was an example of when [REDACTED] would use his personal email to send a message to the Secretary.
4. [REDACTED] could not recall any specific details regarding the fourth email but speculated that it referred to the collating of relevant news clips.
5. In the fifth email the term "Dirty Space" refers to a non SCIF space, where unsecured communications could be used.
6. The sixth email references the Secretary's transition between Blackberry devices. [REDACTED] remembered that her first device was blue in color but he could not recall the make or model. [REDACTED] stated that her second Blackberry was "not blue" but again could not recall any additional details. The second device was remotely activated by COOPER and then [REDACTED] provided it to the Secretary once it was activated. He was unsure if she had additional Blackberry devices thereafter.
7. The seventh email references a photograph that the Secretary took of the reporters traveling with her while they were in Greenland or Iceland. The Secretary wanted to share the photo with the individuals in the picture and asked [REDACTED] to remove any "identifiers" before sending the picture to them. [REDACTED] stated that "identifiers" simply referred to the Secretary's email address as she did not want to inadvertently give out her email address.
8. The eighth email refers to the Secretary's house in Washington, D.C., on Whitehaven St. While discussing the email [REDACTED] provided that he did not recall any other emails being configured on the iPad besides [REDACTED]@gmail.com. Nor did he see her use any other devices to access the clintonemail.com domain, aside from her Blackberry. He did not

b6  
b7Cb6  
b7Cb6  
b7Cb6  
b7Cb6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of [REDACTED] . On 12/31/2015 . Page 4

recall her traveling with a laptop or other personal computers.

9. The ninth email references the switch to a personal office email system that was created after the Secretary left State. [REDACTED] stated that he had no involvement in the process aside from what is described in the email and that he did not have any other interactions with Platte River Networks. He was unsure who secured the hrcoffice.com domain but did not believe that it was [REDACTED] further provided that after leaving State he acted as a paid advisor to the Secretary while she was promoting her book. During this time he used a personal Gmail account until the hrcoffice domain was stood up.

b6  
b7C

(U//~~FOUO~~) [REDACTED] provided that he was not directly involved in culling the Secretary's 60,000 emails aside from reviewing approximately half a dozen emails. In those instances, he was asked to provide the reviewers with additional context about the emails.

b6  
b7C

(U//~~FOUO~~) A copy of the above referenced emails and the original interview notes are attached in a 1A envelope.

~~SECRET//NOFORN~~

FBI INFO  
CLASSIFIED BY: NSICG J37365T94  
REASON: 1.4 (C)  
DECLASSIFY ON: 12-31-2041  
DATE: 08-22-2016

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/22/2016

(U//~~FOUO~~) On June 21, 2016, [redacted] DOB [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] in his [redacted] Washington, DC. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) From January, 2009, until January, 2011, [redacted] was the [redacted] [redacted] at the United States Department of State (DoS). In this capacity, [redacted] reported to [redacted]

b6  
b7C

(U//~~FOUO~~) Following his tenure at DoS, [redacted] worked at the [redacted] [redacted] as a [redacted]. In June of 2012, [redacted] transitioned from the [redacted] to the [redacted] where he served as the [redacted] [redacted] left [redacted] in 2015 for his current position with the [redacted]

b6  
b7C

(U//~~FOUO~~) [redacted] held a Top Secret (TS)/Sensitive Compartmented Information (SCI) clearance while at DoS. He interacted regularly with Secretary of State HILLARY R. CLINTON, and accompanied her on a few international trips. [redacted] was not in direct email contact with CLINTON, and was not aware until recently how much of the information he emailed to her staff was forwarded up to CLINTON. [redacted] recalled knowing CLINTON had a "different" account than others at DoS, but did not know it was a "private" email account.

b6  
b7C

(U//~~FOUO~~) While at DoS, [redacted] "irregularly" attended Deputies Committee (DC) and Principal Committee (PC) meetings. However, [redacted] was present for more PC and DC meetings when he was working [redacted]. The NSC hosted all PC and DC meetings, which were convened by either the National Security Advisor or Deputy National Security Advisor. DoS was not present at every PC or DC meeting. Invitations and attendance depended on the topic. When DoS was invited to a PC or DC meeting, it was not uncommon for the DoS Regional Bureaus to send representation relevant to the topic of discussion.

b6  
b7C

Investigation on 6/21/2016 at Washington, D.C.

b3  
b7E

File # [redacted]-302 Date dictated N/A

By SA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~SECRET//NOFORN~~



Continuation of FD-302 of Interview of [REDACTED], On 6/21/2016, Page 2

(S//NF) [REDACTED]

b6  
b7Cb1  
b3  
b6  
b7C

(U//FOUO) [REDACTED] was familiar with the [REDACTED] Report," and recalled [REDACTED] was tasked with conducting a policy review of Afghanistan and Pakistan early in President OBAMA's administration. [REDACTED] did not recall how many different versions of the [REDACTED] Report were generated.

b6  
b7C

(U//FOUO) Agents asked [REDACTED] to review an email and attachment dated 10/4/2009 and with the Subject: "draft" and an attachment title "Pak Paper 10-03dc.docx." After reviewing the email and attachment, [REDACTED] explained he vaguely remembered the period of time surrounding the email, but did not specifically recall the email or attachment. [REDACTED] assessed he would not have been one to write the document attached to the email, and believed it was likely drafted by somebody in the Special Representative to Afghanistan and Pakistan's (SRAP) Office. [REDACTED] would have likely been one of the final reviewers of the document, describing himself as the "Clean up guy." [REDACTED] who was in the DoS Policy Planning Office, may have also been involved in drafting the document.

b6  
b7C

(U//FOUO) Agents drew [REDACTED] attention to the fact that information contained in the referenced 10/4/2009 email attachment also appeared as SECRET//NOFORN in a March, 2009, version of the [REDACTED] Report. [REDACTED] did not know who at DoS would have ultimately determined the classification of the document. [REDACTED] assessed either CLINTON or someone in her front office would have classified the document. [REDACTED] believed CLINTON and RICHARD HOLBROOKE would have at least read the contents of the report prior to finalization. Specific information contained in the report was publically discussed at the time, so in [REDACTED] opinion, the document was not classified. Much of the information contained in the report was originally based from various contributors' expertise; therefore it would not have been classified. He further stated that while he had no visibility into the DoS classification approval chain, [REDACTED] assessed the report might have been considered Unclassified while it was a working document, and later classified when it became an official record. It also could have been marked classified because almost all documents intended for the NSC are classified for transmission.

b6  
b7C

(S//NF) [REDACTED]

b1  
b3  
b6  
b7C

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of \_\_\_\_\_ Interview of [REDACTED] \_\_\_\_\_ On 6/21/2016, Page 3

b6  
b7C

b1  
b3

(U//~~FOUO~~) Notes of the interview and the documents displayed for [REDACTED] will be maintained in an FD340 envelope and filed with the captioned investigation.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/25/2015

(U//FOUO) On 11/23/2015, [REDACTED] was interviewed in his office at the [REDACTED] by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and [REDACTED]. After being advised of the identity of the interviewing agents, and the nature of the interview [REDACTED] provided the following information:

b6  
b7C

(U//FOUO) From 2010 through 2012, [REDACTED] served as the [REDACTED] [REDACTED] in the Department of State (DoS) Bureau of Near Eastern Affairs (NEA). [REDACTED] oversaw the office which focused on DoS interests in North Africa. [REDACTED] was the DoS senior level expert on [REDACTED]

b6  
b7C

(U//FOUO) [REDACTED] did not directly communicate with Secretary of State HILLARY R. CLINTON, in fact, [REDACTED] did not recall ever communicating directly with any Secretary of State. [REDACTED] did not recall ever communicating directly with CLINTON's executive staff. [REDACTED] may have exchanged an email with CLINTON's Chief of Staff for Public Affairs, JACOB SULLIVAN, on one or two occasions. [REDACTED] did not recall ever communicating directly with CLINTON's Chief of Staff for Operations, CHERYL MILLS.

b6  
b7C

(U//FOUO) [REDACTED] interfaced with DoS executive management predominately through his superiors in NEA. [REDACTED] would communicate to Deputy Assistant Secretary (DAS) JANET SANDERSON and RAY MAXWELL or Assistant Secretary JEFFREY D. FELTMAN, who was later replaced by BETH JONES.

b6  
b7C

(U//FOUO) [REDACTED] and NEA management had separate computer terminals for handling Unclassified and Classified materials.

b6  
b7C

(U//FOUO) During his tenure as the [REDACTED] was on the phone daily with the then Ambassador of Libya, CHRISTOPHER J. STEVENS, who was later killed in the September 12, 2012 attacks on the U.S. consulate in Benghazi, Libya. [REDACTED] would come into work early and talk to STEVENS on the phone. [REDACTED] and STEVENS would communicate through both open and classified means of communication. However, the classified communication capabilities were limited in Libya.

b6  
b7C

---

Investigation on 11/23/2015 at Washington, D.C.File # [REDACTED]-302 Date dictated N/Ab3  
b7EBy SA [REDACTED] SA [REDACTED]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED] On 11/23/2015 Page 2b6  
b7C

(U//FOUO) Following his conversations with STEVENS [REDACTED] would orally brief the NEA DAS. If the information was particularly time sensitive, [REDACTED] would sometimes write an email. [REDACTED] assumed the NEA DAS briefed up whatever information they deemed important from [REDACTED] briefings to SULLIVAN and/or MILLS. Questions regarding the information [REDACTED] provided came back down through his chain of command. [REDACTED] did not recall ever being directly questioned by CLINTON, MILLS or SULLIVAN regarding any of his reporting.

b6  
b7C

(U//FOUO) [REDACTED] was not aware CLINTON was using a private email account not assigned by DoS, nor did [REDACTED] have knowledge that CLINTON's email was hosted on a private, non-DoS, server. [REDACTED] did not recall ever receiving a direct email from CLINTON, other than an email or two that would have been sent to the entire DoS. [REDACTED] only learned of CLINTON's private email and server when the story broke in the Press earlier this year.

b6  
b7C

(U//FOUO) Agents asked [REDACTED] to review an email [REDACTED] dated 11/18/2012 with the Subject line "FYI – Reports of arrests – possible Benghazi connection." The email was shown to [REDACTED] as it was released by DoS FOIA office, and as it appeared on the DoS Reading Room. [REDACTED] noted that the email was sent on a Sunday evening, and it would not have been unusual for [REDACTED] to be in his office during that time. [REDACTED] assessed that he likely sent the email from the office, but sent it via unclassified email, as most of the people who needed to be briefed on the information were not in the office and did not have access to classified communications at the time.

b6  
b7C

(U//FOUO) The individuals [REDACTED] addressed the email in question to were as follows:

b6  
b7C

BETH E. JONES, Assistant Secretary NEA  
RAYMOND D. MAXWELL, Deputy Assistant Secretary NEA

[REDACTED]

b6  
b7C

(U//FOUO) [REDACTED] noted that [REDACTED] and [REDACTED] spoke nearly daily during [REDACTED] tenure as [REDACTED]. The two would converse via high side email or orally. [REDACTED] assessed that the information he typed in the email concerning [REDACTED] was received via an unclassified telephone conversation. He further assessed [REDACTED] received the information from the RSO or Legal Attaché (LEGAT) visiting from Cairo.

b6  
b7C

(U//FOUO) [REDACTED] had no knowledge of his email being forwarded, but assumed that the individuals he emailed direct would either forward the information on to the appropriate executives or

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED]. On 11/23/2015. Page 3

b6  
b7C

brief them orally [REDACTED] noted that in general if information is sent to SULLIVAN, he assumed it would be forwarded or briefed to CLINTON.

b6  
b7C

(U//~~FOUO~~) [REDACTED] noted that some of the language contained in the email may have later been classified, but due to special circumstances surrounding the situation at the time he received the information, there was a necessity to share the information quickly.

b6  
b7C

(U//~~FOUO~~) [REDACTED] kept notes with his calendar, and may have recorded some information concerning the call that preceded the email in question. [REDACTED] indicated he would attempt to locate his calendar/notes from that time period if requested.

b6  
b7C

(U//~~FOUO~~) [REDACTED] interacted with the DoS Ops Center a few times a week during the Libya crisis. The Ops Center would set up management level conference calls. DoS's Crisis Management Group was also collocated in the Ops Center during the crisis in Libya.

b6  
b7C

(U//~~FOUO~~) [REDACTED] prefers oral briefings over email, and noted he did not grow up in the age of email. [REDACTED] does not mark his DoS emails for the record, but maintains an archive of his personal DoS email account when his mailbox fills up and he needs to free-up more space.

b6  
b7C

(U//~~FOUO~~) [REDACTED] never used a non-DoS email account for work related communications.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was never asked to move something from the high side to the low side in a way that seemed inappropriate.

b6  
b7C

(U//~~FOUO~~) Agents notes are maintained in a 1A envelope.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/25/2016

(U//~~FOUO~~) On May 24, 2016, HEATHER SAMUELSON, Date of Birth (DOB) [REDACTED], was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at the law offices of Wilkinson Walsh + Eskovitz, 1900 M Street NW, Suite 800, Washington, DC. Present for the interview was SAMUELSON's counsel, Beth Wilkinson, Partner, Alexandra Walsh, Partner, and Hal Brewster, Associate. Also present was FBI Section Chief Peter Strzok, as well as [REDACTED] and [REDACTED] from the Department of Justice (DoJ) Counterintelligence and Export Control Section. After being advised of the identities of the interviewing agents and the purpose of the interview SAMUELSON provided the following information:

b6  
b7C

(U//~~FOUO~~) SAMUELSON is currently serving as a personal attorney for HILLARY CLINTON. She previously worked at the Department of State (DOS) during CLINTON's tenure as the Secretary of State. SAMUELSON initially worked as an assistant in the White House Liaison Office at DOS and then was promoted to the head of the office. SAMUELSON had infrequent interaction with CLINTON while she was at DOS and primarily interacted with CHERYL MILLS. Following the completion of CLINTON's tenure, SAMUELSON worked for one year in the office of the White House Counsel before becoming CLINTON's personal attorney.

(U//~~FOUO~~) SAMUELSON held a TS/SCI security clearance while she was at DOS. She maintained the clearance when she left DOS and still holds the clearance today. SAMUELSON's clearance was reinvestigated in 2014 per standard procedures. SAMUELSON received training on the handling of classified information when she received her clearance and after the reinvestigation but she did not recall the specifics of the training. SAMUELSON did not receive training on the Freedom of Information Act (FOIA) or the Federal Records Act while at DOS. However, she did receive training on the Presidential Records Act while she was at the White House. SAMUELSON did not receive any specific guidance on what documents she should retain when she left DOS.

(U//~~FOUO~~) SAMUELSON provided that she only received two emails from CLINTON while she was at DOS; one on her birthday and another following the death of SAMUELSON's grandmother. SAMUELSON did not become aware of CLINTON's use of a private email account and server until she was serving as CLINTON's personal attorney.

---

Investigation on 5/24/2016 at Washington, DCFile # [REDACTED]-302 Date dictated N/ABy SA [REDACTED] bh SA [REDACTED]b3  
b7Eb6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of Interview of Heather Samuelson, On 5/25/2016, Page 2

(U//~~FOUO~~) SAMUELSON had no contemporaneous knowledge of the decision to transition from the private server in Chappaqua, NY to the services of Platte River Networks (PRN). Nor did SAMUELSON have contemporaneous knowledge that an archive of CLINTON's emails was created by MONICA HANLEY following CLINTON's tenure at DOS. SAMUELSON did not know the location of the laptop, or thumb drive, containing the archive created by HANLEY.

(U//~~FOUO~~) SAMUELSON knew CLINTON transitioned her email to an @hrcoffice.com domain following her tenure at DOS. SAMUELSON believed no old emails were transferred from the @clintonemail.com to the new domain. SAMUELSON did not know how CLINTON or HUMA ABEDIN accessed old emails after the new domain was established.

### Request from DOS

(U//~~FOUO~~) SAMUELSON provided that she was not involved in the initial discussions with DOS regarding the production of records from CLINTON's tenure. SAMUELSON believed DOS had noticed gaps in its records and had reached out to CLINTON, and other former Secretaries of State, to request that they produce any relevant records in their possession. MILLS spoke with the department about this request in late July or early August 2014 and then asked SAMUELSON to assist with the effort. MILLS also received a formal letter from DOS Under Secretary PATRICK KENNEDY, in October 2014 regarding the request.

(U//~~FOUO~~) To SAMUELSON's knowledge DOS did not provide any formal guidance on how to conduct the search aside from indicating that it was CLINTON's responsibility to assess which products were work related and which were personal. SAMUELSON stated that DAVID KENDALL and others from Williams & Connolly LLP served as external representation for CLINTON in this matter.

### Collection of Relevant Emails

(U//~~FOUO~~) SAMUELSON had no emails that were responsive to the DOS request before she contacted PRN. In late July or early August of 2014 she requested PRN provide all emails from CLINTON's tenure that were sent to, or received from, a ".gov" email address [redacted] of PRN, extracted the relevant files and then transferred them to SAMUELSON. To transfer the files, [redacted] sent SAMUELSON an email link that gave him access to her computer after she clicked on it. [redacted] then downloaded the email files onto her laptop and configured them so she could access the password protected emails via Microsoft Outlook. SAMUELSON described herself as "technically deficient" and stated she was near her computer while this transfer occurred but she did not pay close attention to what he was doing. She did not recall the name of the file he transferred to her computer, the location on her computer where it was placed, or if [redacted] took any steps to encrypt the file before transferring it.

b6  
b7c

(U//~~FOUO~~) SAMUELSON was not aware of how [redacted] queried the files or what mailboxes on the PRN server were searched. More specifically, she did not know if the emails were taken

b6  
b7c

Continuation of FD-302 of Interview of Heather Samuelson, On 5/25/2016, Page 3

from the live mailbox or from the HRC archive that had previously been provided to PRN by HANLEY. SAMUELSON stated that she just asked PRN for the ".gov" emails and [REDACTED] gave them to her.

b6  
b7c

(U//~~FOUO~~) In late September or early October of 2014, SAMUELSON requested that PRN provide a full export of all of the emails from CLINTON's tenure to ensure they captured all relevant emails. SAMUELSON stated this request was not done in response to any identified gaps, but in an effort to produce all relevant emails. [REDACTED] provided the full export to SAMUELSON using the same remote access process as described above. While providing the full email export to SAMUELSON, he removed the previously provided ".gov" emails. Upon realizing this SAMUELSON asked [REDACTED] to give her the ".gov" export files again because she wanted to use it as the starting point for her collection of responsive records. Upon receiving the ".gov" export for a second time, SAMUELSON noticed that some of the emails from the initial export were no longer included. SAMUELSON recalled that there seemed to be a pattern with the missing emails and it involved ".gov" addresses that were in the carbon copy (CC) line of the email. SAMUELSON again contacted PRN and requested that they provide the missing documents and in response [REDACTED] provided several smaller .pst exports to fill the identified gaps.

b6  
b7c

(U//~~FOUO~~) SAMUELSON had requested PRN pull all emails from Clinton's tenure, January 2009 to February 2013. However, upon receiving the above described exports she noticed emails were missing for the period of January 2009 to March 2009. She asked PRN to double check for emails from that time period but they were unable to locate any responsive emails. SAMUELSON came to believe that those emails were not backed up on any server and had only resided on the Blackberry CLINTON was using at that time, thus making them un-retrievable. SAMUELSON did not have contemporaneous knowledge of the Apple server and therefore did not make an effort to check it for relevant records. In searching for other relevant records, SAMUELSON checked the [REDACTED]@gmail.com account and found one email exchange. SAMUELSON did not contact other associates of CLINTON, to include HANLEY, to request any records they might have.

b6  
b7c

(U//~~FOUO~~) SAMUELSON was shown a PRN invoice #37068, dated August 16, 2014, which contains the work description "Worked with Heather via phone/remote session to restore access to archived emails per CDM." In response, SAMUELSON stated that she did not know what that work description meant and that she didn't recall ever losing access to the exported emails, aside from when the initial ".gov" export was removed by [REDACTED]

b6  
b7c

(U//~~FOUO~~) SAMUELSON was shown an internal PRN email from [REDACTED] referencing an urgent phone call with CESC on November 24, 2014, to which she provided she had no recollection of what the call was about. SAMUELSON was then shown a PRN work ticket report from November 24, 2014, which contains the summary note "Worked with Heather via phone/remote control session on more specific export requirements." In response, SAMUELSON stated she could not speculate on what those notes meant and she was unaware of any activities by PRN to "re-establish connection to HRC emails" in November of 2014.

b6  
b7c



Continuation of FD-302 of Interview of Heather Samuelson, On 5/25/2016, Page 4

(U//~~FOUO~~) SAMUELSON was never given direct access to the mailboxes on the server and she was not aware of anybody else being granted such access. SAMUELSON was never given administrative access to the server and she was not aware of anybody else being granted administrative access.

### **Cull and Review of Emails**

(U//~~FOUO~~) SAMUELSON stated she was primarily responsible for conducting the review at the direction of MILLS and KENDALL. She conducted the review over the course of several months and completed it just prior to December 5, 2014, when the documents were turned over to DOS. SAMUELSON conducted the review on her laptop, both in her apartment and in MILLS' office in Friendship Heights, Washington DC.

(U//~~FOUO~~) SAMUELSON reviewed the emails provided by PRN in Microsoft Outlook and placed any responsive emails in a separate folder. She began by adding all of the ".gov" emails and any email to or from a ".mil" email address to the folder. She then searched the emails provided by PRN for any email to or from senior leadership at DOS. This included key individuals such as Under Secretaries, Assistant Secretaries, Ambassadors, Department Heads, and Senior DOS Aides. SAMUELSON then reviewed the sender and receivers of the remaining emails to identify any congress members, foreign leaders, or other official contacts. Lastly, she searched the remaining emails for key words that included terms such as Afghanistan, Libya, and Benghazi.

(U//~~FOUO~~) SAMUELSON reviewed the sender, receiver and subject line of every single email during the review. However, she stated that she did not read the content of each individual email if she could determine it was a work or personal email from the sender, receiver or subject line. SAMUELSON provided that she did her best to review and identify any emails that were potentially a mix of work and personal content. When asked how work related emails between ABEDIN and CLINTON may have been missed, SAMUELSON stated ABEDIN may have kept emails that CLINTON did not.

(U//~~FOUO~~) SAMUELSON did not have a formal process for removing duplicate copies of the same email from the set of work related emails. She did not ask PRN to assist with this process. SAMUELSON stated she would remove a copy of the email if she noticed that it was a duplicate but she did not have a formalized or consistent process for identifying and removing duplicates.

(U//~~FOUO~~) Upon completing the review, SAMUELSON printed all of the emails she deemed to be relevant. The paper copies were then subsequently reviewed by MILLS and KENDALL and anything they deemed not to be work related was shredded. The remaining physical documents were ultimately provided to DOS. SAMUELSON stated that she printed the emails in MILLS' office and noted there is still a printer in MILLS' office but she was not sure if it was the same printer.

(U//~~FOUO~~) Following the review, SAMUELSON created a digital copy, or a "preservation copy," of the relevant documents that were provided to DOS. The files were placed on a thumb drive and provided to KENDALL. SAMUELSON believed this drive is the same thumb drive provided to the FBI by KENDALL. SAMUELSON also created a second copy of the documents provided to DOS and placed

Continuation of FD-302 of Interview of Heather Samuelson, On 5/25/2016, Page 5

them on a second laptop of hers. SAMUELSON was not aware of any other copies of the files. Nor was she aware of a master copy of all of the personal and private emails.

(U//~~FOUO~~) SAMUELSON was shown copies of the thumb drives previously provided to the FBI but could not recall if any were the same as the one she had used. One of the thumb drives was labeled as "HC PRIME 2" and SAMUELSON did not know what the label referred to.

(U//~~FOUO~~) The review methodology was developed by SAMUELSON, MILLS and KENDALL. SAMUELSON did not consider using any commercially available e-discovery tools for the review and they did not consult any individuals who were not "an agent of Clinton" during the review process. SAMUELSON stated they did not discuss how to handle potentially classified emails during the review because they had no reason to believe any classified material was contained in the emails. She further noted that none of the emails were marked as being classified.

(U//~~FOUO~~) During the review process SAMUELSON noticed the imported emails displayed CLINTON's email as hrod17@clintonemail.com despite the fact this address was not created until after CLINTON's tenure. SAMUELSON discussed the issue with [REDACTED] but she did not fully understand his explanation for why this was occurring and he was never able to resolve the problem. SAMUELSON did not consult anybody else about this issue.

b6  
b7c

### Deletion of Emails

(U//~~FOUO~~) In January of 2015, SAMUELSON asked [REDACTED] to remove the exported emails files that had previously been provided to her by PRN. While she retained separate digital copies of the emails provided to DOS, as discussed above, she no longer wanted the email exports provided by PRN on her computer. Using a similar process as described above, [REDACTED] accessed her computer remotely and removed the files. SAMUELSON provided that [REDACTED] took additional steps during the deletion process so the files would not be recoverable. SAMUELSON did not know what software or processes were used by [REDACTED] but believed that the files would be difficult, if not impossible, to recover. SAMUELSON did not remember having any discussions with [REDACTED] about deleting relevant data from the free space of her laptop. Nor did she recall any discussions with [REDACTED] about the use of "BleachBit." SAMUELSON did not recall deleting any of the files by herself before contacting PRN.

b6  
b7c

(U//~~FOUO~~) SAMUELSON stated that in May of 2015 she deleted some emails from her copy of the work related emails that were previously provided to DOS. SAMUELSON explained that she was notified by DOS, prior to the release of the first tranche of FOIA emails, that some of the work related emails they had turned over were classified. She was instructed by DOS to delete the files and then empty those files from the trash bin. SAMUELSON did not believe these files were removed from the thumb drive she had previously provided to KENDALL.

(U//~~FOUO~~) In or about December of 2014, SAMUELSON was on a call in which the email retention policy was discussed. She was aware the retention period was changed to 60 days and any older

Continuation of FD-302 of Interview of Heather Samuelson, On 5/25/2016, Page 6

emails would be deleted. However, SAMUELSON did not direct PRN to remove any exported .pst files on the server or any mailboxes on the server.

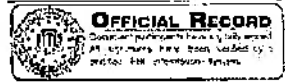
(U//~~FOUO~~) SAMUELSON was not aware of any other deletions of relevant emails. She was aware PRN traveled to the datacenter in March of 2015, via her role as counsel, but had not instructed them to do so. SAMUELSON was not aware of exports or deletions conducted by PRN on the server in September of 2015.

### **Devices used During the Review**

(U//~~FOUO~~) SAMUELSON used her own laptop to conduct the review and noted that she also used the laptop for other work related matters as well. She described it as a Lenovo Yoga 2 laptop. SAMUELSON stated that following the review she accidentally spilled water on the laptop. Fearing that the computer would fail, she purchased a second Lenovo laptop and placed a copy of the emails that were prepared for DOS on it. SAMUELSON noted that the Lenovo Yoga 2 computer continued to work until sometime last year when it failed to power on. The Lenovo Yoga 2 computer is currently in the possession of her counsel and the second Lenovo was given to KENDALL and then subsequently turned over to the FBI. SAMUELSON reviewed pictures of the laptops that were previously turned over to the FBI and stated that the silver Lenovo laptop appeared to be the same as the laptop that she used.

(U//~~FOUO~~) SAMUELSON stated that both laptops were connected to the internet and they both had antivirus software installed on them. SAMUELSON did not repurpose the laptops after the review and never attempted to reformat or factory reset the computers.

(U//~~FOUO~~) A copy of the original interview notes are enclosed in a 1A envelope.

ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIEDUNCLASSIFIED//~~FOUO~~DATE 08-18-2016 BY C28W34B64 NSICG **FEDERAL BUREAU OF INVESTIGATION**Date of entry 06/07/2016

MARCEL LEHEL LAZAR (LAZAR), also known as (AKA) "GUCCIFER", date of birth [REDACTED] alien registration number [REDACTED] was interviewed at the UNITED STATES ATTORNEY'S OFFICE (USAO), 401 Courthouse Square, Alexandria, Virginia 22314. LAZAR was advised that the nature of this interview was to discuss the extent of LAZAR's hacking activities related to HILLARY CLINTON's (CLINTON) personal email server. After being advised of the identities of the interviewing Agents and the nature of the interview, LAZAR provided the following information:

b6  
b7C

LAZAR began by stating that he had never claimed to hack the CLINTON server. SA [REDACTED] then advised that FOX NEWS had recently published an article which reported that LAZAR had claimed to hack the CLINTON server. LAZAR then stated that he recalled the interview with FOX NEWS, and that he had lied to them about hacking the CLINTON server. SA [REDACTED] then asked LAZAR to provide a complete explanation of his hacking activities surrounding the CLINTON server. LAZAR provided the following information in response:

b6  
b7C

On or about March 14, 2013, at approximately 6:00 AM [Romanian Time], LAZAR was perusing [REDACTED] address book. Within it, LAZAR identified an AMERICA ONLINE (AOL) email account of [REDACTED]@aol.com, which he later determined to be the personal email account of SIDNEY BLUMENTHAL. LAZAR then made several attempts to access BLUMENTHAL's email account. After approximately 20 minutes, LAZAR was able to successfully gain access to the account by correctly answering an account security question, which in turn allowed him to reset the password for the account. LAZAR then utilized the new user credentials to access BLUMENTHAL's account.

b6  
b7C

LAZAR recalled that BLUMENTHAL's account contained approximately 30,000 emails, which took him approximately six to seven hours to sort and review. LAZAR downloaded approximately 25 attachments that were contained in the emails, including memorandums (memos) and briefing documents. He recalled that some of those attachments were official memos between BLUMENTHAL and CLINTON. Additionally, LAZAR took screenshots of other items in the account that he deemed to be of interest. LAZAR recalled taking a screenshot of an email that contained information related to the Benghazi incident.

UNCLASSIFIED//~~FOUO~~Investigation on 05/26/2016 at Alexandria, Virginia, United States (In Person)File # [REDACTED] Date drafted 06/02/2016by [REDACTED] [REDACTED] [REDACTED]b3  
b7Eb6  
b7C

UNCLASSIFIED//~~FOUO~~Continuation of FD-302 of (U//~~FOUO~~) Interview of Marcel Lehel LAZAR, On 05/26/2016, Page 2 of 4b3  
b7E

[REDACTED]

While looking through BLUMENTHAL's account, LAZAR identified one email exchange between BLUMENTHAL and CLINTON, where CLINTON was using the domain of clintonemail.com. LAZAR reviewed the header information for that email in attempt to identify the originating IP address for the mail server associated with that domain. LAZAR identified one corresponding IP address, which was 127.0.0.1. LAZAR recognized that IP address as being an internal routing address and assumed that it was assigned to an internal mail server at the AOL service provider. Therefore, LAZAR had no additional information about the CLINTON email server, and concluded his hacking attempts against it at that time. LAZAR stated that this was the full extent of his hacking activities related to the CLINTON email server.

After spending approximately six or seven hours in BLUMENTHAL's account, LAZAR took a break from the computer which lasted approximately two to three hours. When he returned to the computer, he no longer had access to BLUMENTHAL's account. LAZAR recalled that his access was terminated around 8:00 AM [REDACTED] Time. He assumed that BLUMENTHAL likely made a phone call to AOL in order to reset his password and regain access to the account. LAZAR believed that BLUMENTHAL resided in [REDACTED] at that time.

b6  
b7C

As a form of normal practice, LAZAR would send the results of his hacking activities to news agencies world-wide. After accessing BLUMENTHAL's account, LAZAR contacted [REDACTED] at THE SMOKING GUN and advised that he was going to send the BLUMENTHAL information to approximately 100 different news agencies, which he had identified prior to the compromise of BLUMENTHAL's account.

b6  
b7C

LAZAR recalled using a variety of computer hacking tools for his hacking activities, such as ANGRYIP, METASPLOIT, SUBSEVEN, and CAIN AND ABLE. LAZAR used a remote administration tool (RAT) as well, to create his own malware. That tool operated by splitting an existing malware exploit into two pieces, manipulating the hexadecimal code, and then repacking the malware for deployment. LAZAR recalled using the SUBLEGEND7 tool for this activity. LAZAR utilized this technique to send out spear-phishing emails to various targeted victims. The malware would ultimately install a key-logging software on the victim computer.

When asked to elaborate on the key-logging software, LAZAR stated that he could not. When asked how he retrieved the results of the key-logging software from the victims, LAZAR provided that the software allowed him to enter a return email address and the results of the key-logger were emailed to that account. LAZAR could not recall the email accounts that he used for this activity. LAZAR sent this form of malware to approximately 100 different people and estimated that only approximately 15

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~b3  
b7EContinuation of FD-302 of (U//~~FOUO~~) Interview of Marcel Lehel LAZAR , On 05/26/2016 , Page 3 of 4

of them ultimately opened the attachment. LAZAR did not send any spear-phishing emails to users at the clintonemail.com domain.

During other hacking quests, LAZAR utilized various IP scanning tools to determine whether or not an IP address was online and which ports they made available on the Internet. LAZAR recalled using the ANGRYIP scanning tool most frequently. LAZAR attempted to use Russian proxy servers for his scanning activities in order to evade monitoring by the United States government. Russian IP proxies afforded him with faster Internet speeds than others. LAZAR repeatedly checked his outfacing IP address in order to ensure that he was using Russian proxies.

When asked how he utilized Russian proxies with the ANGRYIP tool, LAZAR relayed that the tool itself afforded the ability to connect to Russian proxies. LAZAR could not provide any additional details on how the ANGRYIP tool accomplished this.

When asked about other Internet proxy usage, LAZAR provided that he also utilized MOZILLA FIREFOX as his browser of choice, and that a plug-in was available for the browser which routed Internet traffic through Russian proxies. LAZAR could not provide any additional details on how the plug-in accomplished this, nor could he recall the plug-in that he used in FIREFOX. LAZAR also used the HIDEMYASS website for masking his online activities as well.

In the beginning of the interview, LAZAR recalled using the METASPLOIT tool in approximately 2008 or 2009. He stated that he was merely an amateur with METASPLOIT and that he really didn't understand how to use it. LAZAR utilized METASPLOIT on WINDOWS computers only, from a graphical user interface (GUI) rather than the WINDOWS command prompt. LAZAR is not familiar with the LINUX operating system. Later in the interview, LAZAR recalled using METASPOIT in either 2009 or 2010, during which time frame he made a how-to FACEBOOK video that demonstrated how one could take a remote screenshot of a user's desktop with METASPLOIT.

LAZAR utilized the CAIN AND ABLE software tool for password cracking. He also used that tool from a GUI rather than the command prompt. LAZAR recalled that the GUI had green and red buttons on it. When asked to describe how he utilized the CAIN AND ABLE program, LAZAR stated that he would use it for password cracking once inside a network. When asked whether or not he used it for cracking password hashes that were dumped from a system he replied yes. When asked to further describe the process of dumping password hashes from a system, LAZAR provided that he could not do

UNCLASSIFIED//~~FOUO~~

UNCLASSIFIED//~~FOUO~~b3  
b7EContinuation of FD-302 of (U//~~FOUO~~) Interview of Marcel Lehel LAZAR, On 05/26/2016, Page 4 of 4

[redacted]

so in English. When asked whether or not he could describe that process in Romanian, he stated that he could not. LAZAR used the CAIN AND ABLE software product in either 2010 or 2011.

LAZAR used other remote administration tools for his hacking activities, but could not recall the names of any of them. When targeting an IP address for access LAZAR often attempted to log into it via his web browser, by typing the IP address into the browser. LAZAR utilized multiple different computers for his hacking activities, none of which he has access to anymore. LAZAR recalled working with computers since he was approximately 15 years old.

On approximately four or five occasions during this interview, LAZAR referred to himself as being an amateur hacker and not a professional. On one occasion, LAZAR also referred to himself as being a "script kiddie", who merely knows how to hack accounts by answering security account questions correctly, as he did with the BLUMENTHAL account.

Present during this interview were the following individuals: LAZAR, FBI SA [redacted], LS [redacted], FBI SA [redacted], DSS SA [redacted], [redacted], DOJ CCIPS [redacted], AUSA [redacted], AUSA [redacted] and LAZAR's Attorney, Public Defender [redacted]

b6  
b7CUNCLASSIFIED//~~FOUO~~

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/30/2015

(U//~~FOUO~~) On December 22, 2015, BRYAN PAGLIANO was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and Information Technology Specialist/Forensic Examiner [REDACTED] at the offices of the Department of Justice's Counterintelligence and Export Control Section (CES). Also present, were AkinGump attorneys [REDACTED] [REDACTED] Connor Mullin, Counsel and Mark MacDougall, Partner. Additionally, [REDACTED] and [REDACTED] from the U.S. Department of Justice were also present. After being advised of the identities of the interviewing agents, and the purpose of the interview, PAGLIANO provided the following information:

b6  
b7C(U//~~FOUO~~) PAGLIANO [REDACTED]b6  
b7C

[REDACTED] HILLARY

CLINTON, PAGLIANO came to work on HILLARY CLINTON's 2008 presidential campaign as an information technology specialist. Following HILLARY CLINTON's appointment as the Secretary of State in 2009, PAGLIANO gained employment at the Department of State (DOS) as an Information Technology Specialist in the Bureau of Resource Management.

(U//~~FOUO~~) In the fall of 2008, JUSTIN COOPER introduced himself to PAGLIANO via email and subsequently called PAGLIANO. In the call, COOPER stated he understood PAGLIANO was liquidating computer equipment from HILLARY CLINTON's 2008 presidential campaign and explained he was interested in transitioning from an Apple OS X private email server used by aides of BILL CLINTON to another email exchange server. COOPER asked PAGLIANO for help setting up new equipment to support a new email server and for assistance in the administration of the server. PAGLIANO began work on building an email server at K street using computer equipment from HILLARY CLINTON's 2008 presidential campaign. In late 2008, at the time PAGLIANO was building the server, he did not know HILLARY CLINTON would be Secretary of State or have an account on the server. PAGLIANO believed the email server he was building would be used for private email exchange with BILL CLINTON aides.

(U//~~FOUO~~) Around March 2009, once the new server equipment was assembled, COOPER and PAGLIANO met at the CLINTON residence in Chappaqua, NY to install the server and migrate the email

Investigation on 12/22/2015 at Washington, D.C.b3  
b7EFile # [REDACTED]-302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b6  
b7C



Continuation of FD-302 of Interview of Bryan Pagliano, On 12/22/2015, Page 2

accounts from the Apple OS X server to the new server. PAGLIANO also recalled that [REDACTED] was present, as well as some United States Secret Service (USSS) Special Agents. PAGLIANO recalled the Apple OS X server to be in the basement at Chappaqua and consisting of an Apple Power Macintosh G4 or G5 tower and an HP printer supported by Internet Printing Protocol (IPP) over port 9100 so that staff could print from the Harlem office. PAGLIANO installed the new server equipment which was comprised of a 12-unit (12U) rack with a Dell PowerEdge 1950 used as a Blackberry Enterprise Server (BES), Dell PowerEdge 2900, Dell unmanaged switch, 3U power supply, 3 terabyte (TB) external hard drive, Kiwi Syslog Server, and a Cisco Private Internet eXchange (PIX) 515E IP firewall (the collection of server equipment hereafter referred to as Exchange Server 1). PAGLIANO stated that he did not utilize tape backups but implemented "disk-to-disk" backups instead. PAGLIANO began the email migration from the Apple OS X server to Exchange Server 1 while on-site in Chappaqua in March 2009, but did not finish on-site and continued working on the migration from his hotel room. PAGLIANO believed he "popped out" all the email from the Apple OS X server when migrating and that no email content should have existed on the Apple OS X server once it was migrated to Exchange Server 1. COOPER changed the Mail Exchange (MX) records to ensure delivery to Exchange Server 1. There were only two system administrators on Exchange Server 1, PAGLIANO and COOPER. PAGLIANO disagreed with housing Exchange Server 1 in a residential basement due to having only one unreliable internet connection. COOPER disagreed and wanted physical access to Exchange Server 1. PAGLIANO never knew of Exchange Server 1 residing in another physical location other than Chappaqua.

(U//~~FOUO~~) As far as the Apple OS X server is concerned, PAGLIANO did not know of any other function or use of the server, other than to facilitate email exchange. PAGLIANO did not know who installed the Apple OS X server, but believed COOPER was the only person with administrator access. Two email domains existed on the Apple OS X server, presidentclinton.com and clintonemail.com. Both domains were also maintained on Exchange server 1. PAGLIANO believed [REDACTED] COOPER, [REDACTED] and [REDACTED] had email accounts on the presidentclinton.com domain, and HUMA ABEDIN and [REDACTED] had email accounts on the clintonemail.com domain. Once email was migrated to Exchange server 1, all users could use either the presidentclinton.com or clintonemail.com domains for receiving email but replies would be sent from the clintonemail.com domain for users of the clintonemail.com domain. PAGLIANO did not know if HILLARY CLINTON had an account on the Apple OS X server, but he did not migrate one. PAGLIANO did not know how users connected to the Apple OS X server. [REDACTED] or COOPER would monitor the printer linked to the Apple OS X server, but PAGLIANO was unaware what, if anything, it was used for. PAGLIANO believed the people with physical access to the Apple OS X server was anyone who had access to the basement at the CLINTON residence. [REDACTED] had physical access, but not administrative access, to the OS X server. Sometime after the email migration from the Apple OS X server to Exchange server 1 was complete, COOPER discussed repurposing the Apple OS X server with PAGLIANO. PAGLIANO believed the intention was for the Apple OS X server to be installed as a workstation somewhere in the basement in Chappaqua for use by either COOPER or [REDACTED]

b6  
b7cb6  
b7c

Continuation of FD-302 of Interview of Bryan Pagliano, On 12/22/2015, Page 3

(U//~~FOUO~~) PAGLIANO requisitioned the hardware for Exchange Server 1 from a datacenter at HILLARY CLINTON's presidential campaign headquarters at 4420 W. Fairfax Drive, Arlington, Virginia. He recalled the PowerEdge 2900 to have been a Microsoft SQL server and PAGLIANO did not recall if he wiped the drives of the hardware used to build Exchange Server 1. PAGLIANO made the decision to use a Microsoft Small Business Server (SBS) environment on Exchange Server 1 since he had used it before and assessed it would be perfect for a small amount of users exchanging email. Exchange Server 1 was only used for email exchange, and although PAGLIANO did enable Windows SharePoint Services, it was never used. PAGLIANO wanted to use a cloud service similar to that used in HILLARY CLINTON's 2008 Presidential campaign, but COOPER disagreed with PAGLIANO and did not want to use a cloud service. Because of this decision, PAGLIANO used an external hard drive to back-up Exchange Server 1 using Windows back-up service. To effect this change, PAGLIANO scheduled a task through Windows for a full back-up once a week and a differential back-up every day. These periodic back-ups would overwrite on the hard drive in a first-in, first-out manner. For security, PAGLIANO used Microsoft Forefront on the Dell PowerEdge 2900 as a baseline security analyzer. PAGLIANO recalled finding a virus, but recalled no other detail, other than it being nothing of great concern. PAGLIANO chose to turn File Transfer Protocol (FTP) off.

(U//~~FOUO~~) PAGLIANO thought the biggest vulnerability to Exchange Server 1 to be a Brute Force Attack (BFA). PAGLIANO stated that BFAs increased over the life of the server and he set-up the logs to alert COOPER of a failed log-in attempt. The Internet Protocol (IP) filtering on the server was manual using a 515E straight IP block and PAGLIANO used Domain Name System (DNS) for inbound filtering. On the Dell PowerEdge 1950, PAGLIANO used a Kiwi Syslog server and tried to pull and review the firewall log files once a month. At some point, COOPER put PAGLIANO in contact with [REDACTED] from the USSS for a reason unknown to PAGLIANO. [REDACTED] told PAGLIANO to also perform outbound filtering of email traffic.

b6  
b7c

(U//~~FOUO~~) The back-up hard drive and mailboxes on Exchange server 1 were not encrypted. PAGLIANO wanted to move toward two-factor authentication using an RSA authentication server for all Remote Desktop Protocol (RDP) access on Exchange Server 1 because he thought it was a good practice. As a test, PAGLIANO installed it on his workstation, as well as COOPER's, but PAGLIANO did not end up implementing two-factor authentication and did not turn off RDP access. PAGLIANO stated there were no security breaches on Exchange Server 1, but there were a lot of BFAs. PAGLIANO knew the attempts were BFAs instead of users forgetting their passwords because the user names in the BFA attempts weren't even close to any legitimate user name. PAGLIANO could not recall a specific country that would attempt an inordinate amount of BFAs.

(U//~~FOUO~~) In summer 2009, PAGLIANO noticed an account on Exchange server 1 called "H." PAGLIANO asked COOPER who this email account belonged to and COOPER stated it belonged to HILLARY CLINTON. PAGLIANO assumed the account was a personal email account. PAGLIANO

Continuation of FD-302 of Interview of Bryan Pagliano, On 12/22/2015, Page 4

recalled the email account to be HDR22@clintonemail.com. Later, after SYDNEY BLUMENTHAL's email account was hacked, HILLARY CLINTON's account changed to HROD19@clintonemail.com.

(U//~~FOUO~~) In summer 2009, [ ] and [ ] both Information Technology Specialists at the DOS, contacted PAGLIANO and asked him to come to the 7<sup>th</sup> floor in DOS Headquarters. Once there, PAGLIANO was asked if he was aware of the clintonemail.com domain and PAGLIANO replied in the affirmative. PAGLIANO recalled nothing further about this encounter. PAGLIANO relayed this incident to [ ] and [ ] had a "visceral" reaction and didn't want to know anymore. In late 2009 or early 2010, [ ] reached out to PAGLIANO again and relayed to PAGLIANO that the use of a private email server by HILLARY CLINTON may be a federal records retention issue. [ ] relayed to PAGLIANO that he wanted to convey this to HILLARY CLINTON's inner circle, but could not reach them and asked if PAGLIANO would relay this information. PAGLIANO then approached CHERYL MILLS in her office and relayed [ ] concerns regarding federal records retention and the use of a private email server. PAGLIANO remembers MILLS replying that former Secretaries of State had done the same thing, to include COLIN POWELL. PAGLIANO thought he may have also mentioned the federal records retention issue with JUSTIN COOPER. Additionally, PAGLIANO recalled a third conversation with [ ] where [ ] brought up security concerns and stated that email transiting from a state.gov account to Exchange Server 1 should be through a Transport Layer Security (TLS) tunnel. [ ] stated to PAGLIANO that he wouldn't be surprised if classified information was being transmitted.

b6  
b7c

(U//~~FOUO~~) PAGLIANO stated the hardware used for Exchange Server 1 was paid for by the CLINTON family and through the 2008 presidential campaign and at least some of the hardware was acquired through US21 Computers. PAGLIANO believed most financial and acquisition matters regarding the CLINTONs would go through COOPER directly. PAGLIANO performed work for the CLINTONs without a contract and through contact with COOPER. COOPER wanted to do work under a retainer, but they settled on an hourly wage.

(U//~~FOUO~~) In June 2011, PAGLIANO travelled to Chappaqua to perform maintenance and install new upgrades to Exchange Server 1. The discs began failing in the 3 TB external hard drive in Exchange Server 1 and PAGLIANO replaced it with a CISCO NAS storage device. PAGLIANO chose CISCO because they make good products and he may have consulted US21 Computers as well. PAGLIANO allocated more than half of the storage space for back-ups of Exchange Server 1 and the rest for file storage. When uninstalling the 3 TB hard drive and installing the CISCO NAS, PAGLIANO did not move the contents from one to the other. PAGLIANO simply unplugged the USB connection for the 3TB hard drive and pointed the server back-ups toward the CISCO NAS. PAGLIANO also added memory to the Dell PowerEdge 1950, added a Gigabit switch, upgraded to a CISCO ASA 5500 firewall, off loaded syslogging to the CISCO NAS, bought a CISCO botnet filter and CISCO Intrusion Prevention Service (IPS) and replaced the batteries on the UPS along with other various upgrades and maintenance. Additionally, PAGLIANO upgraded the BES from 5.0 to 6.0 and checked for any software patching.

Continuation of FD-302 of Interview of Bryan Pagliano, On 12/22/2015, Page 5

(U//~~FOUO~~) In the Winter of 2011, the Internet Service Provider (ISP) providing internet service to the CLINTON residence in Chappaqua went down due to a storm. As a result, Exchange Server 1 was unable to process email. While the Internet was down, and to ensure email delivery, PAGLIANO advised COOPER to change the mail exchanger (MX) record for email accounts on Exchange Server 1 to point to Google. PAGLIANO wasn't certain if COOPER did this or who it was done for, but assumed it was done for HILLARY CLINTON and HUMA ABEDIN since they were the most concerned about lack of email delivery.

(U//~~FOUO~~) Individuals with an email account on Exchange Server 1 could log into their account through any means available to them. PAGLIANO viewed his responsibilities as maintenance and operation of the server. PAGLIANO recalled HILLARY CLINTON used a BlackBerry as a mobile device, but could not recall the various handsets. PAGLIANO met with MONICA HANLEY at some point in 2011 or 2012 to configure a BlackBerry for HILLARY CLINTON, but could not recall any detail about the device.

(U//~~FOUO~~) Upon [redacted] leaving the CLINTON's employ and pursuant to a request from [redacted] PAGLIANO recalled doing an export of 40 Gigabytes of [redacted] email. This is the only export PAGLIANO could recall doing. PAGLIANO believed he may have done an export of email for [redacted] but could not recall. PAGLIANO did recall doing an import of DOS contacts for HUMA ABEDIN onto Exchange Server 1.

b6  
b7C

(U//~~FOUO~~) PAGLIANO could not recall accessing the content of email on Exchange Server 1 and was never aware of any classified information residing on Exchange Server 1.

(U//~~FOUO~~) In early 2013, PAGLIANO recalled the user limitations and reliability of Exchange Server 1 prompted discussions to search for another vendor to manage a CLINTON email exchange server. PAGLIANO recalled a conversation with [redacted] and COOPER about [redacted] [redacted] career aspirations and what email requirements she may need. Eventually, MILLS and [redacted] weighed in relating to Exchange Server 1 and the end of HILLARY CLINTON's tenure as Secretary of State. At some point, an individual named [redacted] began the process of finding a vendor to manage a new CLINTON email exchange server. PAGLIANO did not know [redacted] previously, or how she came to be involved with the search for a vendor. Eventually [redacted] showed PAGLIANO a presentation detailing three vendors and their capabilities. PAGLIANO recommended a company called Platte River Networks (PRN). Ultimately, PAGLIANO recalled the decision being with [redacted] and she chose PRN.

b6  
b7C

(U//~~FOUO~~) Once the decision was made to go with PRN, PAGLIANO recalled communicating with PRN employee [redacted] related to the transition from Exchange Server 1 to the server PRN was going to use. Around this time, PAGLIANO was already 4 to 5 months into a new job as an IT

b6  
b7C

Continuation of FD-302 of Interview of Bryan Pagliano, On 12/22/2015, Page 6

specialist at GARTNER. PAGLIANO gave [ ] administrator access to Exchange Server 1 as well as user names and passwords to individual email accounts. PAGLIANO recalled talking to [ ] once or twice and possibly, [ ]. In order to prepare Exchange Server 1 for the transition to PRN, PAGLIANO also "trimmed" mailboxes and cleared out white space. PAGLIANO described this as a maintenance process of reclaiming space from old mailboxes, like in the example of [ ]

b6  
b7C

(U//~~FOUO~~) Based on conversations he had or was aware of, PAGLIANO recalled knowing that PRN was going to use a DATTO service for backing up their server, a CloudJacket device for network protection, and potentially, two-factor authentication. [ ] was responsible for establishing the contract of services PRN was going to implement and ensure they were implemented.

b6  
b7C

(U//~~FOUO~~) PAGLIANO was shown an email dated January 30, 2014 where a user list was populated by Platte River Networks regarding their management of a CLINTON email server. Regarding the email, PAGLIANO did not recognize the mailbox "HRC Archive." PAGLIANO stated after PRN took control of managing an email server for the CLINTONS, he had no visibility into the server or the mailboxes.

(U//~~FOUO~~) In what PAGLIANO remembered as the fall of 2013, MILLS called PAGLIANO and inquired about the effectiveness of two types of software for wiping computer data, but PAGLIANO could not recall the names of the software. PAGLIANO discussed the difference between "bit" wiping and deleting with MILLS. PAGLIANO inferred from his conversation with MILLS that PRN was going to excise data. PAGLIANO recalled using Boot and Nuke software when deleting and repurposing computers while working on HILLARY CLINTON's 2008 presidential campaign, but didn't recall if he discussed that with MILLS.

(U//~~FOUO~~) In July 2014, PAGLIANO had a conference call with MILLS and [ ] to discuss an archive of HILLARY CLINTON emails from her time as Secretary of State. PAGLIANO recalled that MILLS and [ ] were trying to determine why a gap existed in HILLARY CLINTON's emails between January 2009 and March 2009. In separate conversations with COOPER, PAGLIANO understood that CLINTON used a BlackBerry email address before hosting her account on Exchange Server 1 and that explained the gap from January 2009 to March 2009. PAGLIANO could not recall a conversation with MILLS or [ ] after July 2014.

b6  
b7C

(U//~~FOUO~~) In Spring 2015, MILLS asked PAGLIANO if he would mind talking to DAVID KENDALL from Williams & Connolly LLP. PAGLIANO agreed to talk to KENDALL and described the interaction as a shorter version of PAGLIANO's conversation with FBI agents as memorialized herein. PAGLIANO stated there is nothing he told KENDALL that he didn't also relay to the interviewing FBI agents.

Continuation of FD-302 of Interview of Bryan Pagliano, On 12/22/2015, Page 7

(U//~~FOUO~~) At this point in the interview, FBI agents displayed documents to PAGLIANO that were Bates stamped as an identifying mark. PAGLIANO was asked questions as it pertained to each respective document. The following was provided by PAGLIANO:

(U//~~FOUO~~) After viewing a document marked HC-001, PAGLIANO stated the credit of \$5,000.00 to his account was a payment, including expenses, for his work in March 2009 setting up Exchange Server 1. The payment of \$8,350.83 in June 2011 was for his previously described maintenance work on Exchange Server 1, to include expenses.

(U//~~FOUO~~) After viewing a document marked HC-014, PAGLIANO stated the line item "1/11/2011 Conference call with Security team" was the previously described communication with [REDACTED] related to outbound filtering. PAGLIANO stated [REDACTED] was an individual he worked with at US21 Computers. PAGLIANO recalled HILLARY CLINTON turned off Bluetooth capability on her BlackBerry, while COOPER, and possibly [REDACTED] enabled Bluetooth on their handsets.

b6  
b7C

(U//~~FOUO~~) PAGLIANO stated [REDACTED] referred to in a document marked HC-023, was [REDACTED]  
[REDACTED]

b6  
b7C

(U//~~FOUO~~) After viewing a document marked HC-008, PAGLIANO stated the "Mailbox kick off" indicated in the invoice was related to the previously described work exporting [REDACTED] mailbox.

b6  
b7C

(U//~~FOUO~~) After viewing a document marked HC-004, PAGLIANO stated the iPad referred to in the invoice belonged to HILLARY CLINTON. PAGLIANO did not configure the iPad and could not recall when HILLARY CLINTON started using it, nor any other details related to the iPad.

(U//~~FOUO~~) After viewing a document marked HC-010, PAGLIANO stated in March 2013, MILLS requested an analysis of Exchange Server 1. PAGLIANO recalled giving Exchange Server 1 a B+ grade and conveyed in his analysis the limitations of Exchange Server 1 and recommendations for a more robust email system. PAGLIANO relayed the greatest liability of Exchange Server 1 to be reliability and referenced the incidents in which the ISP lost power and was unable to provide internet service to the residence in Chappaqua. PAGLIANO had always been against housing a server in a residential basement and preferred the security and reliability of an established data center. MILLS did not have an email account on Exchange Server 1 and used state.gov and gmail for email exchange.

(U//~~FOUO~~) After viewing a document marked HC-002, PAGLIANO stated the virtual private network (VPN) referred to in the invoice was not for users of Exchange Server 1 and just for administrator use. PAGLIANO stated he installed the IPS at the same time the CISCO ASA firewall went in place in June 2011. PAGLIANO fine tuned the IPS over time, fluctuating between turning logging on and off as needed.

Continuation of FD-302 of Interview of Bryan Pagliano. On 12/22/2015. Page 8

(U//~~FOUO~~) The notes of the interview and all aforementioned documents displayed to PAGLIANO will be stored in a FD340 envelope and filed with the captioned investigation.

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/24/2016

(U//~~FOUO~~) On June 21, 2016, BRYAN PAGLIANO, was interviewed telephonically by Federal Bureau of Investigation (FBI) Special Agents (SA) [REDACTED] and Information Technology Specialist/Forensic Examiner [REDACTED]. Also on the call for the interview were AkinGump attorneys [REDACTED] Partner, Connor Mullin, Counsel, Mark MacDougall, Partner and [REDACTED]. Additionally, [REDACTED] from the U.S. Department of Justice was also on the call. After being advised of the identity of the interviewing Agents, and the nature of the interview, PAGLIANO provided the following information:

b6  
b7C

(U//~~FOUO~~) PAGLIANO did not work on the Apple email server, set-up by JUSTIN COOPER for WILLIAM CLINTON aides, and therefore, has no information regarding a Secure Socket Layer (SSL) certificate registered for the Apple server. PAGLIANO did go through the "full registration" process for establishing an SSL certificate on the server he later built, which enabled email to be encrypted while in transit.

(U//~~FOUO~~) Based on a request from COOPER, PAGLIANO built an email server in early 2009 in HILLARY CLINTON's 2008 presidential campaign space on K street. PAGLIANO could not recall the exact address of the building. Once built, PAGLIANO rented a minivan and drove to Chappaqua, New York to install the email server in the CLINTON residence. PAGLIANO could not recall any existing computer systems at the Chappaqua residence, other than the Apple server previously described to the FBI. When designing the network for the server, PAGLIANO left the CLINTON's home internet network separate from the server - leaving it outside his firewall.

---

Investigation on 06/21/2016 at Washington, DCFile # [REDACTED]-302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b3  
b7Eb6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.



Continuation of FD-302 of Interview of Bryan Pagliano, On 06/21/2016, Page 2

(U//~~FOUO~~) PAGLIANO recalled being given a list of user names and passwords that COOPER asked to be transferred from COOPER's Apple server to PAGLIANO's system. PAGLIANO did not recall transferring an account for HILLARY CLINTON and does not know how her account was installed on the server he built. PAGLIANO installed an IP-based printer on this email system with the express intent of allowing the CLINTON office in Harlem to print at the Chappaqua residence. PAGLIANO installed regular updates to software on the email server using "auto patching" every night. PAGLIANO did some work to experiment with two-factor authentication, but did not implement it on the server because it would have been difficult to administer. PAGLIANO changed the name of the built-in Administrator account and eventually disabled it.

(U//~~FOUO~~) PAGLIANO could not recall saving a file called "netstat.txt" When PAGLIANO received a recommendation to do outbound IP filtering from [REDACTED] at the United States Secret Service, he implemented the change.

b6  
b7C

(U//~~FOUO~~) Around January 2011, PAGLIANO recalled a brute force attack (BFA) on the server where COOPER was receiving failed log-in attempt notifications on his email. Because COOPER could not reach PAGLIANO, COOPER "panicked" and shut down the server. PAGLIANO recalled nothing abnormal about this BFA and eventually trained COOPER to insert IP blocks. PAGLIANO made it clear to COOPER he could not administer the server on a day-to-day basis.

(U//~~FOUO~~) After a recommendation by [REDACTED] an employee at STATE DEPARTMENT (hereafter, STATE) to implement Transport Layer Security (TLS) between the CLINTON email server and STATE servers, PAGLIANO did not implement TLS. PAGLIANO understood the CLINTON email server to be a personal email server and did not see a reason for encryption.

b6  
b7C

(U//~~FOUO~~) In early 2013, PAGLIANO found employment at GARTNER and conversations began between CHERYL MILLS, [REDACTED] and [REDACTED] pertaining to hiring a third-party company to administer a CLINTON email server. PAGLIANO could not recall when he gave access to his server to [REDACTED] from PLATTE RIVER NETWORKS (PRN). Once PAGLIANO did grant access to [REDACTED] PAGLIANO did no utility work on the server and was not monitoring it. Although he

b6  
b7C

Continuation of FD-302 of Interview of Bryan Pagliano, On 06/21/2016, Page 3

could not remember a specific date, PAGLIANO believed the last time he accessed the server was around March of 2013.

(U//~~FOUO~~) Notes of the interview will be maintained in a FD340 envelope.

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 12/16/2015

(U//FOUO) [redacted] was interviewed in her office at the [redacted]  
[redacted] Washington, D.C., by Federal Bureau of  
Investigation (FBI) Special Agents (SA) [redacted] and [redacted]. Interviewing agents  
explained the interview was voluntary and [redacted] could stop the interview at anytime. After  
being advised of the identity of the interviewing agents, and the nature of the interview, [redacted]  
provided the following information:

b6  
b7C

(U//FOUO) [redacted]

b6  
b7C

(U//FOUO) [redacted] participated in daily 8:45am meetings with the Secretary of State and  
her executive staff. CLINTON was not always present at said meetings, as she traveled quite a bit.  
However, [redacted] assessed she attended meetings wherein CLINTON was present approximately  
three to six times a week when CLINTON was in town.

b6  
b7C

(U//FOUO) [redacted] did not have a relationship with CLINTON prior to [redacted]  
DoS employment. [redacted] reported directly to CLINTON, but did not email CLINTON directly  
until six to eight months after she began working at DoS. [redacted] was not initially provided  
CLINTON's email address, so when she wanted to send or forward a message to CLINTON, she would  
route it through HUMA ABEDIN. At some point in the first six to eight months of her employment at  
DoS, [redacted] recalled CLINTON responding to one of the messages she forwarded up directly. At  
this point, [redacted] asked ABEDIN if it was okay to go direct with CLINTON, and was granted the  
"privilege." [redacted] explained the privilege of emailing CLINTON direct was not a privilege she  
used lightly. While [redacted] did not have a history of Government Service, she thought it was  
normal for someone in CLINTON's position to have a "gatekeeper system" in place.

b6  
b7CInvestigation on 12/16/2015 at Washington, D.C.File # [redacted]-302 Date dictated N/Ab3  
b7EBy SA [redacted] SA [redacted]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED] On 12/16/2015, Page 2b6  
b7C

(U//FOUO) [REDACTED] could not recall if the emails she directly sent to and from CLINTON were on CLINTON's DoS or private email account. [REDACTED] did not recall seeing CLINTON's actual email address. Rather, when [REDACTED] received or responded to emails from CLINTON, she recalled seeing a single initial. [REDACTED] believed she recalled seeing "S" as the name of the sender when she received direct CLINTON emails during her time at DoS, as [REDACTED] and other DoS executives would refer to CLINTON as "S." [REDACTED] noted that although she is no longer at DoS, she still maintains email contact with CLINTON and now receives emails from CLINTON where the name of the sender is "H." [REDACTED] had no knowledge CLINTON was using her own private server until it was reported in the media.

b6  
b7C

(U//FOUO) [REDACTED] held a Secret clearance while she was at DoS, but rarely worked in the classified realm. While [REDACTED] received access to and training on the use of DoS's classified computer systems, she hardly accessed DoS' classified system. [REDACTED] did not recall ever using her DoS classified email account. [REDACTED] would have been more likely to use his DoS classified email account. [REDACTED] assessed [REDACTED] [REDACTED] almost entirely worked off the DoS' classified system.

b6  
b7C

(U//FOUO) [REDACTED] was asked to review an email dated 9/12/2009 wherein [REDACTED] sent an email titled "For S – for discussion on Afghanistan tomorrow," from her unclassified DoS email account to CHERYL D. MILLS and JACOB J. SULLIVAN's unclassified DoS email accounts. [REDACTED] ABEDIN, and [REDACTED] were carbon copied on the email. While reading through the email, [REDACTED] at one point stated "good Lord," and further stated that the information contained in the email was [REDACTED] writing [REDACTED] was also referenced in the first line of the email).

b6  
b7C

(U//FOUO) [REDACTED] did not recall specifically sending the 9/12/2009 email to MILLS and SULLIVAN, but mentioned she would not have known the information contained in the body of the email. There Afghanistan Review was ongoing at the time of the 9/12/2009 email, and [REDACTED] recalled strong conflicting opinions concerning the role corruption played in the Afghan political strategy. [REDACTED] likely sent [REDACTED] the information in a separate email, which [REDACTED] would have edited before sending to MILLS and SULLIVAN. [REDACTED] likely spoke to [REDACTED] on the phone or in person about the matter before [REDACTED] emailed the information to [REDACTED].

b6  
b7C

(U//FOUO) After reading the 9/12/2009 email, [REDACTED] admitted she was a bit "shocked when she read over the paragraphs labeled #5 and #6." [REDACTED] stated she "wondered to what extent she read... thought through carefully" before she sent [REDACTED] email on to MILLS and SULLIVAN. SULLIVAN had no idea what was meant by "Marja" Op as stated in the paragraph #5, but explained she believed [REDACTED] was proposing ideas rather than revealing them. [REDACTED] further went on to say she wouldn't have recommended kinetic action.

b6  
b7C

b6  
b7CContinuation of FD-302 of Interview of [REDACTED]. On 12/16/2015. Page 3

(U//FOUO) [REDACTED] and [REDACTED] have known each other for many years. [REDACTED] father was a mentor to [REDACTED]. At the time of the 9/12/2009 email, [REDACTED] was working for [REDACTED]. [REDACTED] would talk to [REDACTED] about a variety of issues, as [REDACTED] likely viewed [REDACTED] as a back channel to get information to CLINTON. [REDACTED] described [REDACTED] as a "bold thinker." [REDACTED] saw her role as ensuring CLINTON received a wide range of viewpoints on various topics.

b6  
b7C

(U//FOUO) Agents also asked [REDACTED] if she recalled a 6/3/2011 email she sent regarding a hacking of Google email accounts, in which she recommended using the information as a platform for discussing issues with the DoS Information Technology system. [REDACTED] immediately remembered the email and explained she initially thought it was why the FBI wanted to speak with her.

b6  
b7C

(U//FOUO) [REDACTED] did not recall being advised or instructed against using a personal email account or personal devices. [REDACTED] used her DoS assigned Blackberry. However, she was assigned a DoS Dell computer, which was very dated, so she opted to use her personal laptop when she was out of the office. [REDACTED] was also issued a fob for which to remotely sign onto DoS systems. While [REDACTED] did use the fob on occasions to remotely sign into the DoS system, she explained the system was slow and would shut down while in use. [REDACTED] who resides in [REDACTED] would often sign into and work off of [REDACTED] network from her home, and transfer information she needed back over to DoS systems.

b6  
b7C

(U//FOUO) SULLIVAN was always operating off of his DoS Blackberry, so [REDACTED] doubted he ever used a personal account for DoS business. However, MILLS would sometimes send very early morning emails to [REDACTED] (around 5am) that were sent from a personal Gmail account [REDACTED] believed was [REDACTED]@gmail.com. [REDACTED] could not recall the specific content of emails she received from MILLS' personal email account, but believed their content was mainly instructional.

b6  
b7C

(U//FOUO) [REDACTED] could not recall an instance where a conversation (email or otherwise) was moved from an unclassified to classified space. It would be more common for a conversation to turn "confidential" and the circle of participants would dwindle in size to accommodate sensitivities, rather than change the venue of the conversation.

b6  
b7C

(U//FOUO) [REDACTED] opined that most policy and strategy discussions would be considered unclassified, acknowledging that some of the participants in policy and strategy discussions may have additional details concerning sources and methods that would have come from classified channels.

b6  
b7C

(U//FOUO) At the conclusion of the interview [REDACTED] told agents she had not mentioned the interview to CLINTON or any of contacts from DoS. [REDACTED] further asked if she was allowed

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED]. On 12/16/2015. Page 4

b6  
b7C

to tell SULLIVAN and/or CLINTON she spoke with the FBI, and explained she was concerned they could be upset to learn she spoke with the FBI without telling them. Agents explained that while they cannot prohibit [REDACTED] from referencing the interview, they would prefer [REDACTED] use discretion when discussing the matter, as to prevent unnecessary information from leaking into the press.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was not previously interviewed by DoS or any other entity related to the topics discussed during this interview.

b6  
b7C

(U//~~FOUO~~) Agent notes are maintained in a 1A.

~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/11/2016

(U//FOUO) On February 18, 2016, [ ] DOB [ ] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [ ] and [ ] at the law offices of [ ] Washington DC. Also present for the interview were [ ] of [ ] and Department of Justice (DoJ) Counterintelligence and Export Control Section [ ]. After being advised of the identities of the interviewing agents, and the purpose of the interview, [ ] provided the following information:

b6  
b7C

(U//FOUO) In 2013, [ ] founded [ ] where he continues to serve as the Managing Director. Prior to founding [ ] served as the [ ] to former [ ] and [ ] [ ] also served in various positions on [ ]

b6  
b7C

(U//FOUO) [ ] coordinated frequently with officials from the Department of State (DoS) during his tenure at both the [ ] and [ ] [ ] coordinated with DoS weekly while at he was at [ ] further stated there was close coordination between the [ ] and DoS on all levels. [ ] coordinated more frequently with DoS during his [ ] tenure, as it was necessary to coordinate with DoS on everything that happened "down range."

b6  
b7C

(U//FOUO) [ ] primary DoS contacts while he was both at [ ] and [ ] included CHERYL MILLS [ ] and JACOB SULLIVAN. [ ] also occasionally communicated directly with [ ] and some U.S. Ambassadors when he was assigned to [ ]

b6  
b7C

(U//FOUO) Most of [ ] contact with DoS while at both [ ] and [ ] was via telephone or email. [ ] had classified and unclassified telephones and email systems available on his desk at both [ ] and [ ] When [ ] signed on to his computers at [ ] he was directed to a classified network and would have to switch over to [ ] unclassified network if he wanted to communicate on an open/unclassified system, whereas when [ ] signed on to his [ ] computer, the system automatically defaulted to the unclassified network.

b6  
b7C

(U//FOUO) [ ] could not recall what email account was synced to his [ ] issued Blackberry. [ ] Blackberry while at [ ] was synced to his unclassified [ ] account.

b6  
b7C

Investigation on 2/18/2016 at Washington, DC

b3  
b7E

File # [ ]-302 Date dictated N/A

By SA [ ] SA [ ]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

~~SECRET~~

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 2/18/2016, Page 2

b6  
b7C

(U//FOUO) \_\_\_\_\_ was provided a STE and safe for home use during his \_\_\_\_\_ tenure. \_\_\_\_\_ explained that he did not utilize the safe to store documents, but occasionally used the STE. \_\_\_\_\_ did not leave the STE plugged in at all times, rather he would wait for someone to contact him on an unclassified line and request a secure call from his home before he would physically plug in the STE.

b6  
b7C

(U//FOUO) \_\_\_\_\_ he attended weekly lunch meetings with then Secretary of State HILLARY CLINTON, and \_\_\_\_\_ and CLINTON also met regularly at National Security Council (NSC) Principal Committee (PC) meetings while \_\_\_\_\_ with the CLINTON family, as he served as President WILLIAM J. CLINTON's \_\_\_\_\_ in the 1990's.

b6  
b7C

(U//FOUO) \_\_\_\_\_ never emailed directly with CLINTON. He was not aware of the email account CLINTON was using, nor was he aware that her email account was operating off of a private server. According to \_\_\_\_\_ would not have utilized email as a means to communicate with CLINTON. If \_\_\_\_\_ wanted to contact or convey a message to CLINTON, \_\_\_\_\_ would subsequently contact the aforementioned DoS senior staff (MILLS, SULLIVAN, or \_\_\_\_\_) to relay the appropriate information.

b6  
b7C

(U//FOUO) Agents asked \_\_\_\_\_ to review an email dated 3/21/2009 and with the subject line \_\_\_\_\_ The email was sent from \_\_\_\_\_@gmail.com to "H" (identified as CLINTON's personal email account). The email \_\_\_\_\_

b6  
b7C

b3 per CIA

(U//FOUO) Agents asked \_\_\_\_\_ to review an email dated 12/30/2009 and with the subject line \_\_\_\_\_ The email was sent from \_\_\_\_\_ to CLINTON, and referenced information \_\_\_\_\_ claimed to receive from \_\_\_\_\_ After reading the email, \_\_\_\_\_ explained he recalled the incident referenced in the email and remembered \_\_\_\_\_ when the incident occurred. \_\_\_\_\_ recalled being contacted by an Executive Assistant (EA) \_\_\_\_\_ Last Name Unknown (LNU) who reported the incident in Afghanistan. \_\_\_\_\_ subsequently contacted \_\_\_\_\_ who requested \_\_\_\_\_ notify the President, Vice President, Chairman of the Joint Chiefs of Staff, Secretary of State, and Secretary of Defense. \_\_\_\_\_ contained some anecdotes about the incident. \_\_\_\_\_ could not recall if he received the information from \_\_\_\_\_

b6  
b7C



Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 2/18/2016, Page 3

b6  
b7C

\_\_\_\_\_ LNU via secure phone (STE) or on an open line. \_\_\_\_\_ could not recall the specifics concerning how he relayed the incident to \_\_\_\_\_ but stated most of the calls he made that day concerning the incident were likely on an unclassified line due to the emergency of the situation. He described his role in the call as contacting his counterparts to relay a brief synopsis of the incident with the caveat that his counterparts should "give their boss a heads up." \_\_\_\_\_ further explained he may have participated in follow up calls on the STE, but could not say for sure either way.

b6  
b7C

(U//FOUO) Agents also showed \_\_\_\_\_ an email exchange dated 2/10/2010 with the subject of \_\_\_\_\_ email." In the email chain SULLIVAN contacted \_\_\_\_\_ to ask for \_\_\_\_\_ email address. \_\_\_\_\_ replied that \_\_\_\_\_ email was \_\_\_\_\_@gmail.com. Thereafter, SULLIVAN asked if this email account was the one that \_\_\_\_\_ used for work and \_\_\_\_\_ confirmed that it was. After reviewing the email, \_\_\_\_\_ explained that he primarily used his unclassified \_\_\_\_\_ and \_\_\_\_\_ email accounts respectively for work purposes. However, he noted that he may have used \_\_\_\_\_@gmail.com on occasions when he could not access his official \_\_\_\_\_ or \_\_\_\_\_ unclassified emails.

b6  
b7C

(U//FOUO) \_\_\_\_\_ reviewed another email dated 11/20/2010 with the subject line \_\_\_\_\_ in Israel," in which he sent the email to SULLIVAN on both \_\_\_\_\_@gmail.com and SULLIVAN's DoS unclassified email account. Also on the receiving line of the email were \_\_\_\_\_ and \_\_\_\_\_ via their "nsc.eop.gov" email accounts. \_\_\_\_\_ could not recall why he would have sent the email to SULLIVAN's gmail account, but stated he would normally email SULLIVAN via his DoS account. \_\_\_\_\_ did not recall ever receiving instruction from SULLIVAN or any DoS employee regarding contact on a gmail account rather than their DoS email. \_\_\_\_\_ listed both his \_\_\_\_\_ and \_\_\_\_\_@gmail.com accounts at the bottom of the email because it provided multiple means for people to contact him while he was on travel in the event his work email was not available.

b6  
b7C

(U//FOUO) Agents asked \_\_\_\_\_ to review a fifth email dated 09/11/2012 and with the subject line "Libya." [Note: The email shown to \_\_\_\_\_ was in a redacted format based on a DoS Freedom of Information Act (FOIA) response to Judicial Watch]. After reviewing the redacted email, \_\_\_\_\_ explained there was a series of meeting on 9/11/2012 in \_\_\_\_\_ office concerning the events surrounding Benghazi. The email \_\_\_\_\_ reviewed referenced what \_\_\_\_\_ referred to as a deployment meeting. There are three types of deployment meetings according to \_\_\_\_\_ 1. Deployment orders, which is the standard process of determining who needs to go where 2. "Careful hurry up deployment," which takes place over the course of a couple of days and is quicker than the standard process 3. "On the fly quick reaction" deployment, which is used only in emergency situations. The only time \_\_\_\_\_ could recall the "on the fly reaction deployment" happening was after Benghazi.

b6  
b7C

(U//FOUO) \_\_\_\_\_ was asked to review a sixth email dated 10/30/2012 with the subject line "This am Green on Blue." [Note: The email shown to \_\_\_\_\_ was in a redacted format based on a DoS FOIA response]. \_\_\_\_\_ referenced said email. \_\_\_\_\_ explained he sent the email to rapidly coordinate the Public Affairs responses \_\_\_\_\_ and DoS in regards to the incident referenced in the email. \_\_\_\_\_ and \_\_\_\_\_ were the respective Public Affairs contacts at DoS and \_\_\_\_\_

b6  
b7C

~~SECRET~~

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 2/18/2016, Page 4

b6  
b7C

(U//~~FOUO~~)

[REDACTED]

b6  
b7C

(U//~~FOUO~~) In response to the article, [REDACTED]

b6  
b7C

[REDACTED] However, [REDACTED] stated that he did not say the [REDACTED]  
[REDACTED] because he did not even know if that statement was true.

b1 per CIA  
b3

(U//~~FOUO~~) [REDACTED] did not have any concerns regarding how DoS handled classified information during his tenure at either [REDACTED] or [REDACTED]

b6  
b7C

(U//~~FOUO~~) [REDACTED] indicated he would be available for re-contact if needed.

(U//~~FOUO~~) A copy of the original interview notes and the referenced emails and article are attached in a 1A envelope.

b6  
b7C

~~SECRET~~

~~TOP SECRET~~ [REDACTED] ~~NP~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

# FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/20/2016

b3 Per CIA

(S//NF) On May 19, 2016, [REDACTED] was interviewed by  
Special Agent (SA) [REDACTED] and SA [REDACTED] at the Central Intelligence Agency  
(CIA) in McLean, Virginia. Also present for the interview was [REDACTED] CIA attorney [REDACTED]  
[REDACTED] After being advised of the identities of the interviewing agents and  
the purpose of the interview, [REDACTED] provided the following information:

b6  
b7C

b3 per CIA

b1 per CIA  
b3

b1 per CIA  
b3

b1 per CIA  
b3

b1 per CIA  
b3

Investigation on 05/19/2016 at McLean, VA

File # [REDACTED] Date dictated N/A

b3  
b7E

by SA [REDACTED] SA [REDACTED]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~ [REDACTED] ~~NP~~

b1  
b3

~~TOP SECRET~~

~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

Continuation of FD-302 of Interview of [REDACTED], On 05/19/2016, Page 2 b3 per CIA

b1 per CIA  
b3

b1 per CIA  
b3

b1 per CIA  
b3

b1 per CIA  
b3

~~TOP SECRET~~

~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

b3 per CIA

Continuation of FD-302 of Interview of [REDACTED], On 05/19/2016, Page 3

[REDACTED] was shown a copy of an email from [REDACTED] with the subject [REDACTED]. After reviewing the email he provided that [REDACTED] appeared to be trying to coordinate with DOS but that the email should have been classified [REDACTED]

b1 per CIA  
b3

[REDACTED] was shown a copy of an email from [REDACTED] with the subject [REDACTED]. After reviewing the email he provided that the email should be classified but that he was not surprised that DOS had sent it on an unclassified channel. [REDACTED] further noted that the DOS unclassified email system had previously been penetrated by a foreign adversary.

b1 per CIA  
b3

[REDACTED] was shown a copy of an email from [REDACTED] with the subject [REDACTED]. After reviewing the email [REDACTED] stated that his true name, and that of [REDACTED] should not have been included in an unclassified email. [REDACTED] provided that talking points could be classified or unclassified. They were conveyed from the CIA to DOS via a cable that included a tear line below which the approved talking points were provided.

b1 per CIA  
b3

[REDACTED] was shown a copy of an email from [REDACTED] with the subject [REDACTED]. After reviewing the email [REDACTED] stated that he did not know enough about [REDACTED] to assess if the talking points included in the body of the email were classified or not.

b1 per CIA  
b3

[REDACTED] was shown a copy of an email from [REDACTED] with the subject [REDACTED]. After reviewing the email [REDACTED] provided that any discussion of [REDACTED] should be considered classified.

b1 per CIA  
b3

[REDACTED] was shown a copy of an email from [REDACTED] with the subject [REDACTED]. After reviewing the email [REDACTED] provided that the details [REDACTED] should be classified because [REDACTED]

b1 per CIA  
b3

[REDACTED] concluded the interview by stating that DOS has shown an increased tendency to communicate via email. He believed that they did this for simplicity, to avoid unauthorized disclosures such as Wikileaks, and to prevent other USG partners from seeing their "back channel" discussions. [REDACTED] continued to say that the personnel at DOS were experienced and knew that this information was classified. However, they did it anyways and their actions hurt the CIA and other agencies whose equities were conveyed in the emails.

b1 per CIA  
b3

~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~

~~NF~~

b1  
b3

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 05/19/2016, Page 4

b3 per CIA

(U//~~FOUO~~) A copy of the original interview notes and referenced documents is enclosed in a 1A envelope.

~~TOP SECRET~~

~~NF~~

b1  
b3

~~TOP SECRET~~

b1  
b3

FD-302a (Rev. 10-6-95)

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/29/2016

(U//~~FOUO~~) On March 17, 2016, MICHAEL MORELL [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at the FBI Washington Field Office, 601 4<sup>th</sup> Street NW, Washington DC. Present for the interview was MORELL's counsel, [redacted] Attorney at Law, at [redacted]. Prior to the interview [redacted] agreed to sign a non-disclosure agreement in anticipation of viewing classified documents during the interview. After being advised of the identities of the interviewing agents, and the purpose of the interview, MORELL provided the following information:

b6  
b7C

(U//~~FOUO~~) MORELL joined the Central Intelligence Agency (CIA) in 1980 as an analyst and served in a variety of roles of increasing responsibility before he was named the Deputy Director (DD) in 2010. MORELL was the DD from May of 2010 until August of 2013, during which he served as the Acting Director on two occasions. The first time was in 2011 when LEON PANETTA left and the second was in late 2012 when DAVID PETRAEUS resigned.

(U//~~FOUO~~) As DD, MORELL had regular interaction with the Deputy Secretary of State WILLIAM BURNS during the daily Deputies meeting at the White House. MORELL would also attend meetings at the Department of State (DoS), or have secure telephonic conversations, with BURNS or [redacted] to discuss inter-agency affairs. MORELL never communicated directly with the Secretary of State (Secretary).

b6  
b7C

(U//~~FOUO~~) MORELL did not recall ever having direct communications with JAKE SULLIVAN, because SULLIVAN did not attend the Deputies meeting. Nor did he have direct communications with CHERYL MILLS or HUMA ABEDIN.

(U//~~FOUO~~) MORELL never emailed the Secretary directly and had no knowledge that she was using a private email account and server.

b1 per CIA  
b3

Investigation on 03/17/2016 at Washington DC

File # [redacted] Date dictated N/A

By SA [redacted] SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b3  
b7E

b6  
b7C

~~TOP SECRET~~

b1  
b3

~~TOP SECRET~~

~~NI~~

b1  
b3

Continuation of FD-302 of

Interview of Michael Morell

Date 03/17/2016 Page 2

[REDACTED]

b1 per CIA  
b3

[REDACTED]

b1 per CIA  
b3

[REDACTED]

b1 per CIA  
b3

[REDACTED]

b1 per CIA  
b3

[REDACTED]

b1 per CIA  
b3

[REDACTED] MORELL was shown a copy of an email chain from [REDACTED]  
[REDACTED] with the subject [REDACTED] MORELL did not immediately recall the meeting referenced in the

b1 per CIA  
b3

~~TOP SECRET~~

~~NI~~

b1  
b3



~~TOP SECRET~~ [REDACTED] ~~NP~~

FD-302a (Rev. 10-6-95)

b1  
b3

Continuation of FD-302 of [REDACTED] Interview of Michael Morell , On 03/17/2016 , Page 3

[REDACTED] email [REDACTED] b1 per CIA  
[REDACTED] b3

MORELL stated that he understood why the email would be considered classified but he did not believe that the email would jeopardize any sources, methods, or otherwise compromise national security.

(S//~~NP~~) MORELL was shown a copy of an email chain from [REDACTED] with the subject [REDACTED] MORELL stated that he did not recall the cited article [REDACTED] b1 per CIA  
[REDACTED] b3

[REDACTED] MORELL stated that assuming the email was true, then it would be classified [REDACTED]  
[REDACTED]

(S//~~NP~~) MORELL was shown a copy of an email chain from April of 2011 with the subject "Scots police, UK govt to meet over Libyan defector (Reuters)." MORELL recalled the matter referenced in the email and provided the following context: At the time of the email the Libyan Civil war was raging and MUAMMAR GADDAFI was still in power. Part of the U.S. strategy at that time was to induce the defections of high ranking officials from Libya. In the email chain BURNS expressed that MUSA KOUSSA should be treated well following his defection to support future defections [REDACTED] b1 per CIA  
[REDACTED] but that the CIA would say that the content is classified because [REDACTED] however, MORELL did not feel that the disclosure of this information would cause "horrible" damage. b3

[REDACTED] MORELL was shown a copy of email chains from [REDACTED] b1 per CIA  
[REDACTED] with the subject [REDACTED] MORELL stated that the email discussed [REDACTED] and that it b3  
appeared to be classified as it is absolutely clear that they are referencing [REDACTED]  
[REDACTED] MORELL speculated that SULLIVAN got this information from BURNS or [REDACTED]  
[REDACTED] as he never spoke directly with SULLIVAN regarding [REDACTED] MORELL typically spoke with BURNS about [REDACTED]

[REDACTED] MORELL was shown a copy of an email chain from [REDACTED] b1 per CIA  
[REDACTED] with the subject [REDACTED] MORELL stated that it was clear that they were b3  
discussing [REDACTED] MORELL believed that the email was classified as it discussed operational activities. MORELL initially stated that the content of the email did not "give much away" but he conceded that the [REDACTED] information could potentially be damaging to the operation.

[REDACTED] MORELL was shown a copy of an email chain from [REDACTED] b1 per CIA  
[REDACTED] with the subject [REDACTED] b3  
MORELL stated that it was clear that they were discussing [REDACTED] and the email was likely classified.

~~TOP SECRET~~ [REDACTED] ~~NP~~

b1  
b3

~~TOP SECRET//~~

~~NF~~

b1  
b3

Continuation of FD-302 of interview of Michael Morell, On 03/17/2016, Page 4

(U//~~FOUO~~) MORELL suggested that the interviewing agents talk with leadership from the agency's [redacted] and with leadership from the [redacted] for another assessment of the referenced emails.

b3 per CIA

(U//~~FOUO~~) A copy of the original interview notes and the NDA signed by [redacted] are enclosed in a 1A envelope.

b6  
b7C

~~TOP SECRET//~~

~~NF~~

b1  
b3

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/21/2015

(U//~~FOUO~~) On September 15, 2015, [redacted] Project Manager, Platte River Networks (PRN), office phone [redacted] email address [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted]. Also present for the interview was [redacted] from [redacted] and Department of Justice (DOJ) Attorney [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7c

(U//~~FOUO~~) [redacted] role with the email server project for WILLIAM CLINTON and HILLARY CLINTON, under the account name CESC, involved transporting and installing hardware. He did not serve as the Project Manager, his normal job function at PRN. His first task for the project was to pick up the CESC server and support devices in use prior to PRN being awarded the contract for the project. The server and support devices were located at the CLINTON residence in Chappaqua, NY. In June 2013, [redacted] traveled to New York and drove a rental car to the CLINTON residence. [redacted] contact at the residence, [redacted] Last Name Unknown (LNU), escorted [redacted] to the basement where the equipment was located. [redacted] powered down the equipment and took a Dell PowerEdge 1950 BlackBerry Enterprise Server (BES), Dell PowerEdge 2900 email server (hereafter, predecessor server), Cisco NSS 324 Network Attached Storage Device (NAS), and an external USB hard drive, but left the existing firewall and switch.

b6  
b7c

(U//~~FOUO~~) [redacted] then transported the equipment to an Equinix datacenter in Secaucus, NJ where he reconnected the equipment in the same manner in which it was connected at the CLINTON residence. The goal was to get CESC users back online quickly. [redacted] and [redacted] who was working remotely, then started incorporating new equipment PRN purchased for the CESC project, but [redacted] did not recall if he set it up before or after transporting the server. The new equipment consisted of a Dell PowerEdge 620 server running multiple virtual machines, two new PowerConnect switches, two new Fortinet firewalls, and a DATTO backup device. During this period of time, the predecessor server and new PRN server (hereafter, PRN server) co-existed. The predecessor server had the NAS connected, but it did not appear to be configured for storing any data. The PRN server had a DATTO backup appliance connected to it. After 2-3 days, [redacted] departed Equinix and did not participate in the day-to-day management of the CESC account. Those duties were handled remotely by [redacted]. Several days later, a CloudJacket intrusion prevention device was installed by technicians at Equinix. The CloudJacket was designed to alert PRN and prevent intrusions into the PRN server.

b6  
b7cInvestigation on 09/15/2015 at Denver, ColoradoFile # [redacted]-302 Date dictated N/Ab3  
b7EBy SA [redacted] SA [redacted]b6  
b7c

b6  
b7c

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 09/15/2015, Page 2

(U//~~FOUO~~) In or about March 2015, \_\_\_\_\_ communicated with CHERYL MILLS regarding any existing backups of the CESC email server and the state of the predecessor server. MILLS requested an audit of the existing equipment, but did not direct \_\_\_\_\_ to delete or alter any data found. \_\_\_\_\_ traveled to Equinix datacenter in Secaucus, NJ to conduct an onsite review of the equipment. PRN had migrated all accounts off of the predecessor server by this time, therefore it contained no data. \_\_\_\_\_ reviewed the NAS and external USB hard drive brought from the CLINTON residence as part of the initial transport of equipment. Neither contained any data. While there, \_\_\_\_\_ also took steps to increase security on the system as a result of media articles identifying the existence of the private email server used by the CLINTONS. PRN took these steps without direction from CESC.

b6  
b7c

(U//~~FOUO~~) None of the Internet Protocol (IP) notifications \_\_\_\_\_ reviewed from the CloudJacket device used as part of the security infrastructure for the CESC account were abnormal. All were alerts and some resulted in IP addresses being blocked from accessing the equipment. \_\_\_\_\_ does not believe any nefarious actors got into the system.

b6  
b7c

(U//~~FOUO~~) In or about August 2015, \_\_\_\_\_ traveled to the Equinix datacenter in Secaucus, NJ to turn over the predecessor server to the FBI. Prior to turning over the server, \_\_\_\_\_ powered on the server to check for proprietary PRN software and license copies of other software purchased by PRN. \_\_\_\_\_ recalled removing Magic ISO software because it was expensive and PRN pays for license fees for each copy it uses. \_\_\_\_\_ review of the predecessor server was not requested by CESC.

b6  
b7c

(U//~~FOUO~~) \_\_\_\_\_ never heard anyone from CESC discuss classified information. \_\_\_\_\_ was never asked by anyone from CESC to delete or destroy anything; however, PRN would not have knowledge of individual users deleting content from their accounts.

b6  
b7c

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/04/2016

(U//~~FOUO~~) On February 18, 2016, [redacted] Project Manager, Platte River Networks (PRN), office phone [redacted] email address [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] [redacted] at the offices of Platte River Networks, 5700 Washington Street, Denver, CO. Also present for the interview were SA [redacted] Information Technology Specialist/Forensic Examiner [redacted] [redacted] from [redacted] and Department of Justice (DOJ) Attorney [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

(U//~~FOUO~~) [redacted] handled the technical infrastructure related to the contract PRN had with the Clinton Executive Services Corporation (CESC). [redacted] ran the day to day operations and most direct interactions with the client, including managing and maintaining the Microsoft Exchange email server and associated equipment (collectively hereafter, Server).

b6  
b7C

(U//~~FOUO~~) In March 2015, the CESC requested PRN conduct a complete inventory of data backups and all equipment in PRN's possession related to the services provided to CESC. [redacted] does not recall how or who from CESC communicated this request. In response to the request, [redacted] traveled to the Equinix facility in Secaucus, NJ where the Server housing CESC's data was located. In addition to the currently operating equipment, [redacted] found a Network Attached Storage (NAS) device and an external hard drive that were disconnected. He connected them and reviewed for content, but neither contained any data, so he disconnected them before leaving. [redacted] did not find any unexpected backups during this trip.

b6  
b7C

(U//~~FOUO~~) [redacted] vaguely recalled the name [redacted] from Security Pursuit, but did not know why it was familiar to him. He did not recall implementing any new security protocols in the March 2015 timeframe, but [redacted] did conduct a high level security check of the Server.

b6  
b7C

(U//~~FOUO~~) [redacted] did not recall a backup device of HILLARY CLINTON's connecting via IMAP/SMTP to the Server.

b6  
b7C

---

Investigation on 02/18/2016 at Denver, Coloradob3  
b7EFile # [redacted]-302 Date dictated N/ABy SA [redacted] SA [redacted]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 02/18/2016, Page 2b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ never deleted, nor was he asked to delete the mailbox "hrcarchive" from the Server. He never discussed deleting content, creating .pst files, exports, or shredding of .pst files with \_\_\_\_\_ or anyone else. Additionally, \_\_\_\_\_ is unfamiliar with a program called BleachBit. However, prior to turning over the Server to the FBI, \_\_\_\_\_ removed PRN system tools such as an ISO mounter and, possibly, a monitoring tool from Level Platforms or LabTech.

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/10/2016

(U//~~FOUO~~) On June 10, 2016, JOHN BENTEL, Date of Birth [REDACTED] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED] at the office of [REDACTED] Washington DC. Present for the interview was BENTEL's counsel [REDACTED] Partner [REDACTED] Partner, and [REDACTED] Special Counsel. As well as [REDACTED] from the Department of Justice (DoJ) Counterintelligence and Export Control Section. Prior to the interview BENTEL was [REDACTED] After being advised of the identities of the interviewing agents, and the purpose of the interview, BENTEL provided the following information:

b6  
b7C

(U//~~FOUO~~) BENTEL served at the US Department of State (DOS) for 39 years before retiring in 2012. Most recently, BENTEL was the Director of the Executive Secretariat Information Resource Management (S/ES-IRM) from 2008 until 2012. In this position he reported to LEWIS LUKENS and then to TULINABO (TULU) MUSHINGI. Approximately 85 people were under BENTEL's supervision, including two deputies: [REDACTED] and [REDACTED]

b6  
b7C

(U//~~FOUO~~) BENTEL did not learn that HILLARY CLINTON was using a private email server while she was at DOS until it came out in the press last year. He had no knowledge of the server while he was at DOS. BENTEL met BRYAN PAGLIANO while he was at DOS and knew that he worked for IRM but he did not know that he was also providing support to the CLINTON server.

(U//~~FOUO~~) BENTEL was shown a copy of an email sent from [REDACTED] to BENTEL, [REDACTED] and [REDACTED] on March 17, 2009, with the subject "Secretary Residential Installation Hotwash." BENTEL provided that [REDACTED] was responsible for setting up secure communications in CLINTON's office and residence, and that [REDACTED] was a contractor in [REDACTED] section. After reviewing the email and its attachment, BENTEL stated that he did not recall the email and that he might not have read the email originally because he and his two deputies functioned as "a collective." BENTEL stated that the attachment appeared to be a summary of the communication equipment in CLINTON's residence at the start of her tenure. BENTEL did not know what the "Server: Basement Telephone Closet" listed in the attachment referred to. He then speculated that it might be a server for telephones. Upon further questioning, BENTEL provided that he did not know if DOS used or installed servers to support its telephone equipment.

b6  
b7C

(U//~~FOUO~~) BENTEL was shown an email sent from MONICA HANLEY to HUMA ABEDIN on August 30, 2011 with the subject "HRC blackberry" that referenced a discussion between HANLEY

---

Investigation on 6/10/2016 at Washington, D.C.File # [REDACTED] 302 Date dictated N/ABy SA [REDACTED] SA [REDACTED]b3  
b7E

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

Continuation of FD-302 of Interview of John Bentel, On 6/3/2016, Page 2

and BENTEL. Upon reviewing the document BENTEL provided that he did not recall the email and that he would not have used the term "chapp server." Furthermore, he did not recall CLINTON losing access to her email following Hurricane Irene or any related discussions. BENTEL explained that he did not have a lot of direct interaction with CLINTON's staff and that communication issues would likely be handled by [REDACTED] from the "tech team."

b6  
b7c

(U//~~FOUO~~) BENTEL was aware of the Office of Inspector General (OIG) report from May of 2016 in which it was reported that subordinates raised concerns about the Secretary's server to BENTEL in 2010 and he instructed them not to discuss the matter any further. BENTEL denied that anybody had raised such concerns to him. He further stated that the account provided by the OIG report was inconsistent with his open and welcoming management style.

(U//~~FOUO~~) BENTEL stated that he did not know CLINTON was using a personal email account for DOS business until after it was released in the papers. BENTEL clarified he knew that CLINTON had a personal email account but that he did not know that she was using it for work related matters. BENTEL did not know if CLINTON had a DOS issued email account.

(U//~~FOUO~~) BENTEL was shown an email that he sent to MONICA HANLEY on August 30, 2011 with the subject "Re: S berry." The email discusses a DOS issued email account, SSHRC@state.gov, which had been previously established for CLINTON. In the email, BENTEL wrote that emails on the account would be subject to Freedom of Information Act (FOIA) searches. Upon reviewing the email, BENTEL stated that he did not recall the email exchange or the details surrounding the use of SSHRC@state.gov, noting that the account was likely set up by the system administrator. BENTEL included the caveat about FOIA to make sure that HANLEY was aware of FOIA and that any personal messages on the account would also be subjected to FOIA requests. BENTEL stated his group was not directly responsible for FOIA related matters and that the appropriate contact for FOIA matters within S/ES-IRM was [REDACTED]

b6  
b7c

(U//~~FOUO~~) BENTEL was aware of the State Messaging Archive Retrieval Toolset (SMART) and said it was not used by S/ES-IRM during CLINTON's tenure. BENTEL speculated that it was not rolled out to S/ES-IRM at that time because it was a new system and they wanted to work out any bugs before giving it to the executives. BENTEL stated that STEPHEN MULL would have made the final decision on rolling out SMART to S/ES-IRM.

(U//~~FOUO~~) A copy of the original interview notes and referenced documents are attached in a 1A envelope.



~~SECRET~~

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/7/2016

(U//~~FOUO~~) On December 21, 2015, COLIN POWELL, office address [REDACTED]  
[REDACTED] office phone [REDACTED] was interviewed at his residence by  
Federal Bureau of Investigation (FBI) Special Agent (SA) [REDACTED] and SA [REDACTED]  
[REDACTED] Also present during the interview was [REDACTED] to POWELL.  
After being advised of the identity of the interviewing agents and the nature of the interview, POWELL  
provided the following:

b6  
b7C

(U//~~FOUO~~) In his book, *It Worked for Me: In Life and Leadership*, POWELL wrote a chapter  
called Brainware outlining his efforts to modernize computer systems at the US Department of State,  
hereafter State. When he was sworn in as Secretary of State in 2001, one of the largest problems at State  
was outdated Information Technology (IT) systems. At the time, State and the Central Intelligence  
Agency (CIA) would swap responsibility every 12 months for the communication connections to overseas  
embassies. Sometime thereafter, Congress passed a law establishing a White House agency with the  
responsibility for secure diplomatic telecommunications. POWELL convinced the administration to give  
him time to assess the situation, so he launched a study to determine the agency best suited to maintain  
the communication connections. The study found CIA as the most competent, so POWELL fired State  
and reached an agreement with the then CIA Director GEORGE TENET where POWELL would select  
and evaluate the CIA staff person in charge of the system. Additionally, the system would be based on  
POWELL's requirements.

(U//~~FOUO~~) In 2001, few State employees had a computer at their desks. Typically, there was one  
computer per office, so POWELL budgeted for the purchase of 44,000 computers and put one on every  
embassy desk. The project was done in-house without contractors. To convince and encourage others to  
use computers, POWELL frequently used his to set an example. When traveling to visit embassies, he  
would sit down at a random computer in each embassy and attempt to login to his account. This action  
allowed POWELL to gauge if the embassy staff was maintaining and using their computers.  
Additionally, he would frequently look up Country Notes pages on the State intranet to determine if the  
various bureaus of State were keeping their information up to date. On his desk at State, POWELL had a  
State classified computer and a laptop with a 56kbps modem. The modem was used to access  
POWELL's personal American Online (AOL) account. He viewed his personal email much like a home  
telephone line in that it could be used for personal and business purposes. At times, POWELL would  
correspond with foreign leaders by email. If the conversation became sensitive, whether with foreign  
leaders or other USG personnel, he would arrange for a secure call.

Investigation on 12/21/2015 at [REDACTED]

b6  
b7C

File # [REDACTED] 302 Date dictated N/A

b3  
b7E

By SA [REDACTED] SA [REDACTED]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it  
and its contents are not to be distributed outside your agency.

~~SECRET~~

Continuation of FD-302 of Interview of Colin Powell, On 12/21/2015, Page 2

(U//~~FOUO~~) The IT transformation revolutionized business at State. With a computer on every desktop, the time and space problems were eliminated when sharing information. Prior to the IT deployment, embassies communicated via cables.

(U//~~FOUO~~) The State Inspector General (IG) and Intelligence Community Inspector General (ICIG) both wrote POWELL to ask him if he had any emails from his time as Secretary of State. However, POWELL took no emails with him when he left State and knew of no official record requirements at the time, however, State claimed they were capturing any data necessary. POWELL has not been able to get a straight answer from the federal archives regarding what record requirements were at the time. He is concerned the current environment will discourage open communication and the use of email, ultimately harming US Government efficiency.

(U//~~FOUO~~) When POWELL traveled for State business, a team would put a computer in his hotel room for general use, but he would also have access to State systems. Some threat countries would have additional security requirements such as [REDACTED] If the need arose to have a classified conversation, POWELL would go to a secure facility, such as the local embassy. **b1 per DOS**

(U//~~FOUO~~) In response to reviewing the email attached to this communication in a 1A, POWELL provided the following:

(U//~~FOUO~~) During POWELL's first few weeks at State, he received several security briefings that restricted his ability to communicate. He was admonished that CIA and NSA did not want personal digital assistants (PDAs) inside of SCIFs, even if the PDA did not have wireless capabilities. He requested briefings to explain why PDAs were any more of a risk than the television remote controls in the SCIF, but was not convinced of the risks. As a result of these experiences, he advised HILLARY CLINTON, when she became Secretary of State, to resist restrictions that would inhibit her ability to communicate.

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/21/2015

(U//FOUO) On September 14, 2015, [redacted] Platte River Networks, date of birth [redacted] social security number [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted]. Also present for the interview was Department of Justice (DOJ) Attorney [redacted] and [redacted] attorney at the [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

(U//FOUO) As [redacted] [redacted] described his role at PRN as a general role with the client and not involved with technical details. [redacted] main concern is the general direction of the business.

b6  
b7C

(U//FOUO) Platte River Networks (PRN) worked with an individual named [redacted] to identify business opportunities. In early 2013 [redacted] brought them a client opportunity who she claimed once worked as a public official. After submitting a bid to do the work, PRN became aware the contract they were bidding on was for the management of an email server hosting domains associated with BILL CLINTON, HILLARY CLINTON and their aides. PRN won the bid for the contract and the account was under the name CESC.

b6  
b7C

(U//FOUO) PRN wanted to limit the employees working on the CESC server, so it was determined [redacted] who worked remotely on the server, and [redacted] who handled the server on-site, would be the technical team doing most of the work. [redacted] was aware that PRN picked up an old server from the CLINTON residence and delivered it to Equinix, a datacenter in Secaucus, New Jersey. PRN ordered and installed new server hardware at Equinix and migrated all CESC email from their old server to the new PRN provided server. [redacted] was aware that PRN maintained a back-up of the server known as a DATTO. The DATTO was located at Equinix and worked by taking snapshots of the server and maintaining that data for up to 60 days before it was deleted. [redacted] deferred to [redacted] for specifics. [redacted] was also aware of a BlackBerry Enterprise Server managed by PRN, but deferred to [redacted] on the specifics.

b6  
b7C

(U//FOUO) In or around March 2015 [redacted] was involved in conversations with CESC where they requested to know what email they had, where it was, and how it was backed up. [redacted] and [redacted] handled this request and would know more details. CESC never asked

b6  
b7CInvestigation on 09/14/2015 at Denver, Coloradob3  
b7EFile # [redacted] 302 - 22 Date dictated N/ABy S [redacted] 10/15 SA [redacted] 10/13/2015

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 07/23/2015, Page 2

for administrator rights to the PRN server or for physical access to the server at Equinix. [REDACTED] believed CESC was still a PRN client and were operating under the same contract they originally signed.

b6  
b7C

(U//~~FOUO~~) [REDACTED] didn't believe there was a successful intrusion attempt against the CESC email server run by PRN.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/26/2016

(U//FOUO) On May 23, 2016, [redacted] date of birth [redacted] social security number [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] at the offices of Platte River Networks (PRN) located at 5700 Washington Street, Denver, Colorado 80216. Also present for the interview was [redacted] and via speaker phone [redacted] both attorneys at the [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] was not aware of a laptop containing an archive of email belonging to HILLARY CLINTON that was shipped to PRN around February 2014. [redacted] was not aware what became of the foregoing laptop.

b6  
b7C

(U//FOUO) [redacted] only recently was made aware of a CLINTON email archive file being transmitted to the Clinton Executive Services Corporation (CESC) around July 2014 and September 2014 by [redacted]. [redacted] was not aware of the request by CESC, or transmittal by [redacted] as it was occurring. [redacted] was not aware of what specifically was requested by CESC or exactly how [redacted] fulfilled the request.

b6  
b7C

(U//FOUO) [redacted] was not aware of any support PRN provided the CESC client from October 2014 to January 2015. [redacted] was not aware of any CESC request to delete, wipe or shred their email records. As a [redacted] would not pay attention to technical details of any PRN client.

b6  
b7C

(U//FOUO) At this point in the interview, Agents displayed PRN provided records and email from the March 2015 timeframe. [redacted] provided the following information:

b6  
b7C

(U//FOUO) In March 2015, when various media outlets reported a private email domain and server was used by HILLARY CLINTON, PRN decided to create an internal "share drive" and control access to only the PRN employees working the CESC account. [redacted] stated PRN did have back-ups of their own servers. PRN never deleted information pertaining to the CESC client and provided the FBI all records they maintained pertaining to CESC.

b6  
b7C

Investigation on 05/23/2016 at Denver, Colorado

File # [redacted] 302 - 98 Date dictated N/A

b3  
b7E

By SA [redacted]

SA [redacted]

b6  
b7C

b6  
b7CContinuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 07/23/2015, Page 2

(U//~~FOUO~~) In March 2015, \_\_\_\_\_ stated CESC requested an inventory of all their email content, to include where it existed. PRN employee \_\_\_\_\_ travelled to the Equinix

b6  
b7C

data center in Secaucus, New Jersey where the CESC server equipment was located. \_\_\_\_\_ was not a party to the discussion involving CESC's request for inventory, therefore did not know specific instructions. \_\_\_\_\_ did not recall what \_\_\_\_\_ specifically found on the server equipment.

b6  
b7C

(U//~~FOUO~~) After Agents displayed an email dated March 09, 2015 where CHERYL MILLS discussed preservation of materials, \_\_\_\_\_ could not recall any other request by any entity to preserve CESC related data.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ has no recollection of a conference call on March 25, 2015 or March 31, 2015 with CESC. \_\_\_\_\_ stated CESC never requested their email content be deleted, wiped or shredded. Recently, \_\_\_\_\_ was made aware that \_\_\_\_\_ used Bleachbit software to shred .pst email files containing CESC email content that was transferred to CESC. As \_\_\_\_\_ understood it, \_\_\_\_\_ created a "vehicle" to transfer email files from the live mailboxes of CESC email accounts. \_\_\_\_\_ then later used Bleachbit software to shred the "vehicle" but the email content still existed in the live email accounts.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was unaware of any PRN employee conducting manual deletions of the DATTO device used to back-up the CESC email server.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was unaware of any successful computer intrusion of the CESC server.

b6  
b7C

(U//~~FOUO~~) Notes of the interview and documents displayed to \_\_\_\_\_ will be maintained in a FD340 envelope and filed with the captioned investigation.

b6  
b7C

FD-302a (Rev. 10-6-95)

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/19/2016

(U//~~FOUO~~) On April 19, 2016, [redacted] date of birth (DOB) [redacted] and social security account number (SSAN) [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and [redacted] at the law offices of [redacted] located at [redacted] Washington DC 20005. Also present for the interview were [redacted] attorneys [redacted] and [redacted]. After being advised of the identity of the interviewing Agents, and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] is currently the [redacted] [redacted] met President WILLIAM CLINTON and HILLARY CLINTON when he became an [redacted] at the White House in the fall of [redacted]. After his [redacted] served in various positions in the CLINTON White House and continued to work for President CLINTON after his presidency.

b6  
b7C

(U//~~FOUO~~) In the years after President CLINTON left the White House, CLINTON's staff managed certain details related to the information technology needs of CLINTON's office. One of those needs required negotiating with an individual who owned several .com domains related to CLINTON's name. [redacted] recalled these domains to be presidentclinton.com, clintonfoundation.com, and owjc.com. Ultimately, negotiations were successful and the domains were purchased from the individual.

b6  
b7C

(U//~~FOUO~~) In 2006 or 2007, JUSTIN COOPER obtained a private email server (Apple Server) for the office of President CLINTON. COOPER and [redacted] had several conversations about reliability issues related to the previous outsourced server and decided it would be best to have a server under their physical control at the CLINTON's residence in New York. COOPER handled the procurement and all aspects of server management, to include the creation of new accounts or any requests to move email. [redacted] believed [redacted] and [redacted] initially had email accounts on the Apple Server. [redacted] recalled a conversation with HUMA ABEDIN and COOPER regarding the addition of HILLARY CLINTON to the Apple Server. [redacted] thought it was a bad idea, but the issue had been decided by that point in time. [redacted] believed the addition of HILLARY CLINTON to the Apple Server occurred while she was in the Senate. CLINTON used BlackBerry devices obtained by COOPER to access her email. [redacted] was not involved in the decision to move to a new server (Exchange Server), but recalled it was located, as was the Apple Server, in the basement of the CLINTON's New York residence.

b6  
b7C

Investigation on 04/19/2016 at Washington, DC

File # [redacted] 002 - 70 Date dictated N/A

By SA [redacted] *yph/2016*b3  
b7Eb6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UNCLASSIFIED//~~FOUO~~

Continuation of FD-302 of Interview of Justin Gregory Cooper, On 03/02/2016, Page 2

(U//~~FOUO~~) COOPER notified [ ] few times each year about attempted intrusions of the system, but [ ] could not recall any specific details. They shared a mutual concern [ ] had too much private information about the CLINTONS and may have had access to some of their communications.

b6  
b7C

(U//~~FOUO~~) [ ] had no knowledge regarding the following topics:

b6  
b7C

- discussions to move to the Exchange Server
- personnel involved in the decision to move to the Exchange Server
- domains on the Apple Server or Exchange Server
- users on the Exchange Server
- disposition of the Apple Server or Exchange Server after decommissioning
- classified information on Apple Server or Exchange Server
- conversations concerning federal records as it related to the Apple Server or Exchange Server
- backups of the Apple Server or Exchange Server
- Sensitive Compartmented Information Facilities at the CLINTON's New York or Washington, DC residences [ ] did recall Secure Telephone Units in New York and Washington, DC)
- Secure fax machines or secure computers at the New York or Washington, DC residences

b6  
b7C



-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/09/2016

(U//~~FOUO~~) On June 6, 2016, [redacted] date of birth [redacted] social security number [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] at the FBI Washington Field Office, 601 4<sup>th</sup> Street NW, Washington, DC 20535. Also present for the interview was FBI Intelligence Analyst [redacted]. After being advised of the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] works for [redacted] a defense contractor specializing in the areas of missile, space, and intelligence. In addition, [redacted] owns [redacted] a company focused on domestic data acquisition which [redacted] established in [redacted] has several products to include [redacted] as well as other products drawn from the over 60 billion records in [redacted] possession. [redacted] Dark Horse Data, Inc. (DHD), a company owned by former Deputy Under Secretary of Defense for Intelligence REGINALD HYDE. DHD works with foreign data, can contract directly with the government, and frequently embeds its personnel with clients.

b6  
b7C

(U//~~FOUO~~) In June or July 2015, [redacted] a senior staff member of the United States Senate Committee on the Judiciary, contacted [redacted] out of concerns data from HILLARY CLINTON's email server might end up overseas. Specifically [redacted] wanted to determine if there was an intrusion into CLINTON's server and, if so, whether exfiltrated data fell into the hands of a foreign power. [redacted] was concerned any exfiltrated data could endanger her three sons, who are Marines. Additionally, she was upset as a citizen and Senate Staff Member that this situation could occur. Therefore, [redacted] asked [redacted] if it was possible to determine if CLINTON's server had been compromised. [redacted] stated he would have to look for data that was genuine, authentic, and relevant. [redacted] defined those three terms as follows:

b6  
b7C

- Genuine – data originating from CLINTON's server
- Authentic – data that had not been altered
- Relevant – data from CLINTON's server that was moved outside of the United States to a place where a foreign actor could access it

(U//~~FOUO~~) Since [redacted] did not have funding for the project described above, in August or September 2015 she met with NEWT GINGRICH and asked [redacted] to brief GINGRICH on the project.

b6  
b7C

---

Investigation on 06/06/2016 at Washington, DCb3  
b7E

File # [redacted] 302 - 41 Date dictated N/A

By SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 06/06/2016, Page 2

\_\_\_\_\_ GINGRICH, and \_\_\_\_\_ were all bothered by the potential that data from CLINTON's server had been compromised. GINGRICH wanted to speak with others about the project and in December 2015, recommended \_\_\_\_\_ speak with \_\_\_\_\_ at Judicial Watch. \_\_\_\_\_ briefed the project as four phases to \_\_\_\_\_. The phases were to determine if:

- Phase 1 –CLINTON's server was directly or indirectly attacked
- Phase 2 –SIDNEY BLUMENTHAL's server was directly or indirectly attacked
- Phase 3 – data was exfiltrated outside the United States
- Phase 4 – data was exposed to a foreign actor

As \_\_\_\_\_ briefed the project, he raised the question of what the course of action would be if classified information was uncovered. The three discussed it and decided Judicial Watch's legal counsel should be consulted. \_\_\_\_\_ never received an answer, but was of the opinion that if he uncovered data he thought might be classified, he would be obligated to report it to the appropriate authorities.

(U//~~FOUO~~) In January or February 2016, Judicial Watch's legal counsel advised the project was feasible, but could not involve accessing any systems without authorization. The project could review open source data following the four phases described above. After these initial discussions with Judicial Watch, \_\_\_\_\_ concluded the motivation of Judicial Watch's actions was not centered on the elections.

(U//~~FOUO~~) \_\_\_\_\_ advised there are three potential funding streams for the types of projects his company undertakes. They can be funded by his company, a government contract, or a data arbitrageur. In this situation, the arbitrageur would invest in litigation on the prospect of a judge awarding the arbitrageur attorney's fees.

(U//~~FOUO~~) In February or March 2016, \_\_\_\_\_ company, \_\_\_\_\_ was given \$32,000 by Judicial Watch to proceed with Phase 1. Judicial Watch awarded the contract to \_\_\_\_\_ because they were confident he understood both the Deep Web and Dark Web. After receiving the contract, \_\_\_\_\_ had to determine the best place to obtain the necessary data for the project. Based on the terms outlined by Judicial Watch's counsel, CLINTON and BLUMENTHAL's respective servers were off limits, as were offshore servers. \_\_\_\_\_ turned to \_\_\_\_\_ a former executive at \_\_\_\_\_ a cyber intelligence company which ingests data from the Deep Web and Dark Web and, then, indexes the data. By leveraging \_\_\_\_\_ data, \_\_\_\_\_ could search the Deep Web and Dark Web without exposing his searches to the Internet. \_\_\_\_\_ paid \_\_\_\_\_ \$2,500 to have \_\_\_\_\_ conduct searches based on search terms provided by \_\_\_\_\_. These search terms included, but were not limited to, HILLARY CLINTON, SIDNEY BLUMENTHAL, and an Internet Protocol (IP) address range obtained from an email provided to \_\_\_\_\_ by Judicial Watch. In return, \_\_\_\_\_ provided the results of those searches to \_\_\_\_\_ which was the exclusive data source used by \_\_\_\_\_ for this project.

(U//~~FOUO~~) \_\_\_\_\_ reviewed the data provided by \_\_\_\_\_ and found files from BLUMENTHAL's server on a server in Romania. \_\_\_\_\_ believed BLUMENTHAL had a personal

FD-302a (Rev. 10-6-95)

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 06/06/2016, Page 3

server because he found some of BLUMENTHAL's files on the server in Romania, but not any of BLUMENTHAL's emails. The Romanian server contained approximately 200 Microsoft Word, Excel, and other file types belonging to BLUMENTHAL.

(U//~~FOUO~~) In reference to a May 22, 2009 alleged intrusion of CLINTON's server appearing in a draft version of a report on \_\_\_\_\_'s project \_\_\_\_\_ stated he could not recall where he learned of the hack or the specific date. \_\_\_\_\_ speculated it was possibly from a public report, but he had looked for the source and could not find it. Therefore, \_\_\_\_\_ planned to remove the reference from future iterations of the report.

b6  
b7C

(U//~~FOUO~~) During \_\_\_\_\_'s review of the data obtained by \_\_\_\_\_ he found one sensitive Excel file listing the names of known or suspected jihadists in Libya. \_\_\_\_\_ added that a portion of the file was in Russian. The file did not come from BLUMENTHAL's server, but contained a reference to an IP address range that included the IP address of CLINTON's server. Upon viewing this file, \_\_\_\_\_ became concerned he had found a classified document and stopped the project. This work completed Phase 1 and \_\_\_\_\_ planned to deliver the final report to Judicial Watch soon.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ stated some of the BLUMENTHAL files were dated on or about January 2012, which was the same timeframe when \_\_\_\_\_ contacted \_\_\_\_\_ regarding the Libyan Rogue Nation Judgment Recovery Program (LRNJRP). \_\_\_\_\_ claimed he was hired by the Libyan opposition government to recover the assets of the MUAMMAR GADDAFI government. \_\_\_\_\_ also met with TYLER DRUMHELLER regarding the same matter. \_\_\_\_\_ speculated BLUMENTHAL, if involved in the LRNJRP, could have written the memos as a "shake and bake" tactic.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes and documents provided to the FBI by \_\_\_\_\_ during the interview are enclosed in a 1A envelope.

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/21/2015

On September 14, 2015, [redacted] Platte River Networks (PRN), date of birth [redacted] social security number [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted]. Also present for the interview was [redacted] from [redacted] and Department of Justice (DOJ) Attorney [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

On or about January 2013, [redacted] of [redacted] contacted [redacted] regarding potential business with a high profile former government client. [redacted] had an existing relationship with [redacted] because she previously referred other clients from a family wealth asset management firm. The potential client's current email server architecture lost connectivity during events such as Hurricane Sandy, so they wanted better support than their existing arrangement. [redacted] with the assistance of other PRN personnel, put together a proposal and submitted it to [redacted]. Once PRN was chosen as one of the three finalists for the contract, PRN was notified the potential client was WILLIAM CLINTON and HILLARY CLINTON, doing business through a company named CESC. After PRN won the contract, [redacted] took on a smaller role and [redacted] worked primarily with [redacted] and [redacted]. CESC wanted to keep the number of individuals working on the project small, so PRN identified three people as the only personnel allowed to work directly on the CESC project. Those individuals were identified in a Service Level Agreement (SLA) signed in August 2013 as [redacted] (solution design), [redacted] (project manager), and [redacted] (help desk). [redacted] did approximately 90% of the work for CESC and [redacted] handled approximately 10% of the work. [redacted] role was to help with on-site work at Equinix, while [redacted] handled everything else. [redacted] was ultimately not needed to work on the project.

b6  
b7C

When [redacted] was asked to review an email he sent discussing a new email address for HILLARY CLINTON, [redacted] stated [redacted] could not answer the question for attorney-client privilege reasons. A copy of the email is attached to this communication in an FD-340.

b6  
b7C

PRN chose Equinix as the datacenter for CESC's new email server (hereafter, PRN server) specifically because it did not go down during Hurricane Sandy. This project was PRN's first time using Equinix. [redacted] transported CESC's existing equipment (hereafter, predecessor server) and transported it to Equinix, so the content of the predecessor server could be migrated to the new PRN server.

b6  
b7C

Investigation on 09/14/2015 at Denver, Colorado

File # [redacted]-302-12 Date dictated N/A

b3  
b7E

By SA [redacted] 9/24/15 SA [redacted] 9/30/2015

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 09/14/2015, Page 2

\_\_\_\_\_ stated PRN used an outside firm, MX Logic, for spam filtering, but referred other technical questions regarding spam filtering, data migration, archives/backups, and Microsoft Exchange to \_\_\_\_\_ and/or \_\_\_\_\_

b6  
b7C

\_\_\_\_\_ had no knowledge of:

b6  
b7C

- Email servers used by CESC prior to the one transported by PRN to Equinix.
- The existence of classified information on either server.
- Discussions regarding federal records retention.
- Intrusions to the PRN server.

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/26/2016

(U//FOUO) On May 23, 2016, [redacted] date of birth [redacted] social security number [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] at the offices of Platte River Networks (PRN) located at 5700 Washington Street, Denver, Colorado 80216. Also present for the interview was [redacted] and via speaker phone, [redacted] both attorneys at the [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] for PRN, and in that role, had contact with PRN client CLINTON EXECUTIVE SERVICES CORPORATION (CESC). His points of contact at CESC were CHERYL MILLS, [redacted] and [redacted].

b6  
b7C

(U//FOUO) [redacted] was not aware of a laptop containing an archive of email belonging to HILLARY CLINTON that was shipped to PRN around February 2014. [redacted] was not aware what became of the foregoing laptop.

b6  
b7C

(U//FOUO) [redacted] was not aware of a CLINTON email archive being transmitted to the Clinton Executive Services Corporation (CESC) around July 2014 and September 2014 by [redacted].

b6  
b7C

(U//FOUO) [redacted] was not aware of any support PRN provided the CESC client from October 2014 to January 2015. [redacted] was not aware of any CESC request to delete, wipe or shred their email records.

b6  
b7C

(U//FOUO) At this point in the interview, Agents displayed PRN provided records and email from the March 2015 timeframe. [redacted] provided the following information:

b6  
b7C

(U//FOUO) In March 2015, when various media outlets reported a private email domain and server used by HILLARY CLINTON, [redacted] entertained the idea of hiring a third party company to conduct penetration testing of the CESC email server. [redacted] recommended [redacted] from a company named [redacted] but the testing ultimately did not occur.

b6  
b7C

Investigation on 05/23/2016 at Denver, Colorado

b3  
b7E

File # [redacted] 302 - 94 Date dictated N/A

By SA [redacted]

b6  
b7C

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 07/23/2015, Page 2

(U//~~FOUO~~) In March 2015, [REDACTED] recalled PRN employee [REDACTED] travelled to the Equinix data center, but did not know the purpose of the trip.

b6  
b7C

(U//~~FOUO~~) After Agents displayed an email dated March 09, 2015 where CHERYL MILLS discussed preservation of materials [REDACTED] could not recall any other request by any entity to preserve CESC related data [REDACTED] recalled receiving some guidance by PRN attorneys to preserve data, but could not recall specifically.

b6  
b7C

(U//~~FOUO~~) [REDACTED] had no recollection of a specific conference call on March 25, 2015 or March 31, 2015 with CESC. [REDACTED] did recall conference calls with CESC that were run by PRN's attorney. [REDACTED] stated CESC never requested their email content by deleted, wiped or shredded.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was unaware of any successful computer intrusion of the CESC server.

b6  
b7C

(U//~~FOUO~~) Notes of the interview and documents displayed to [REDACTED] will be maintained in a FD340 envelope and filed with the captioned investigation.

b6  
b7C

FD-302a (Rev. 10-6-95)

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/03/2016

(U//~~FOUO~~) On February 4, 2016, [redacted], home address [redacted] NY, mobile phone [redacted] was interviewed at the law offices of Bryan Cave LLP, 1155 F Street NW, Washington, DC 20004 by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] Department of Justice attorney [redacted] and [redacted] counsel, [redacted] were also present for the interview. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

(U//~~FOUO~~) [redacted] first met President WILLIAM CLINTON and HILLARY CLINTON (CLINTON) in 1997 when he was assigned [redacted] to The White House as [redacted]. At that time, [redacted] received a security clearance after a single scope background investigation was conducted. He served in The White House [redacted] to include traveling with the President, until 2001 when President CLINTON left office. On [redacted] President CLINTON's [redacted] told [redacted] the CLINTONs had been keeping an eye on him and would like him to join their New York family. [redacted] accepted the offer and on [redacted] drove to their Chappaqua, NY residence. For the first six months, [redacted] position was covered as part of the military assistance provided to every president who leaves office. [redacted] He then returned to Chappaqua where he primarily focused on [redacted] but ended up with many more responsibilities.

b6  
b7C

(U//~~FOUO~~) [redacted] recalled an Apple server in the basement of the CLINTON's Chappaqua residence, but does not remember when it was installed or by whom. It was a big box to the right of [redacted] with no external devices attached, however, it had an internal capability to backup data. [redacted] HUMA ABEDIN, [redacted] HILLARY CLINTON, JUSTIN COOPER, AND [redacted] had email accounts under the owjc domain housed on the server. [redacted] also used the server as a workstation.

b6  
b7C

(U//~~FOUO~~) [redacted] did not know of plans to install the server constructed by BRYAN PAGLIANO at the time it occurred. The server consisted of three thin black boxes mounted in a rack. [redacted] described himself as not technical and, therefore, could not speak to any details regarding this server.

b6  
b7C

Investigation on 02/04/2016 at Washington, DC

b3  
b7E

File # [redacted] 302 - 60 Date dictated N/A

By SA [redacted] 3/16/16

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.



Continuation of FD-302 of Interview of [REDACTED], On 02/04/2016, Page 2

(U//~~FOUO~~) [REDACTED] did not recall escorting anyone from Platte River Networks in June 2013 into the Chappaqua residence to remove the server described above.

b6  
b7C

(U//~~FOUO~~) HILLARY CLINTON's office was on the third floor of the Chappaqua residence. After she became the Secretary of State, the State Department (State) converted it into a sensitive compartmented information facility (SCIF). During the installation of the secure lines for the SCIF, [REDACTED] stood at the door as an escort for the technicians. After that conversion, CLINTON was the only one who had the combination to access the office until it was decommissioned one to two weeks after her departure from State. It contained approximately three phones installed by State. [REDACTED] believed all three to be secure phones and described them as a black STU phone, a yellow phone, and a white phone. [REDACTED] did not know the differences in the phones. The office also contained CLINTON's non-secure desktop computer, a shredder, and a secure fax machine. [REDACTED] initially stated he only entered the SCIF once or twice, when CLINTON was present, to remove trash.

b6  
b7C

(U//~~FOUO~~) [REDACTED] later recalled a procedure established by ABEDIN with [REDACTED] at the beginning of CLINTON's tenure at State for situations when CLINTON needed assistance with the secure fax. When [REDACTED] was notified by State personnel of an incoming secure fax, he would locate CLINTON, follow her to the SCIF, and assist as needed with the incoming fax. He was never in the SCIF to receive a fax without CLINTON present and never physically picked up any of the documents received. If the fax was not working, State would sometimes send a courier with documents or a diplomatic pouch to the Chappaqua residence. On those occasions [REDACTED] would escort the courier from the gate to the door and the courier would hand the documents or pouch directly to CLINTON. [REDACTED] would also coordinate the repair of the fax when broken.

b6  
b7C

(U//~~FOUO~~) ABEDIN or CHERYL MILLS would sometimes notify [REDACTED] the Presidential Daily Brief (PDB) would be coming via secure fax to the residence. As described above with other secure faxes [REDACTED] would locate CLINTON and assist with the incoming secure fax. The PDB was also hand carried to the residence on occasion and [REDACTED] would escort the courier to CLINTON.

b6  
b7C

(U//~~FOUO~~) [REDACTED] periodically received emails from ABEDIN with attached documents intended for CLINTON. [REDACTED] would print the documents and give them to CLINTON, but does not know what happened to the documents after CLINTON was finished with them. [REDACTED] Last Name Unknown handled similar duties at CLINTON's residence in Washington, DC.

b6  
b7C

(U//~~FOUO~~) CLINTON had several BlackBerry devices over the course of time. When CLINTON had issues with one of them, [REDACTED] would ask COOPER for advice on how to fix it. [REDACTED] believed CLINTON had a State BlackBerry, but did not recall a secure mobile phone.

b6  
b7C

(U//~~FOUO~~) [REDACTED] did not recall setting up an Apple ID or iPad for CLINTON.

b6  
b7C

(U//~~FOUO~~) [REDACTED] did not recall a secure phone in CLINTON's bedroom.

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 03/23/2016

[redacted], Chief Executive Officer (CEO), was interviewed at his place of employment, [redacted] telephone number is [redacted] and his email address is [redacted] was advised that the FBI had identified 37 login attempts to the APPLE ICLOUD account of hdr22@clintonemail.com, originating from three [redacted]-owned IP addresses. [redacted] was provided with the IP addresses that made the login attempts. After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

[redacted] has approximately [redacted] employees at their main headquarters in [redacted] and an additional [redacted] employees in other locations. [redacted] They provide [redacted]

[redacted] has a large customer base including many US Government agencies and Department of Defense components. [redacted]

[redacted] provided the Agents with a demonstration of the [redacted] on a laptop in his office. [redacted] and others. That data is then [redacted]

[redacted] provides their clients with two basic services: 1) their security platform can be used to link and search for current social media information on the Internet; and 2) [redacted] can provide on-going social media monitoring for their clients. [redacted] explained that the [redacted] utilizes their continuous

Investigation on 03/23/2016 at [redacted]  
File # [redacted] - CYBER - 16 Date dictated N/A  
By SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

monitoring service to generate alerts for new social media posts relating to current [REDACTED]. Additionally, [REDACTED] provides that same service for all United States Department of Commerce employees, whether they are aware of it or not.

b6  
b7C  
b7E

Along with searching for [REDACTED]

b4  
b6  
b7C

[REDACTED] confirmed that two of the three IP addresses shown to him belong to [REDACTED]. [REDACTED] stated that the third IP address may have been assigned to them in the past, but that it was no longer active. The [REDACTED] is assigned to [REDACTED]

b4  
b6  
b7C

[REDACTED] does not maintain historical logs for searches that are conducted by their clients. [REDACTED]

b4  
b6  
b7C

then showed the Agents a screen on his laptop, where the username field was displayed without a corresponding password field.

To the best of [REDACTED] recollection, [REDACTED] was not hired by HILLARY CLINTON or anyone on her behalf. [REDACTED] attributed the login attempts to being conducted by one of their clients, utilizing the [REDACTED] platform. [REDACTED] then left the interview for a brief moment in order to verify that [REDACTED] was not conducting any continuous monitoring services for HILLARY CLINTON. When he returned, [REDACTED] confirmed that they are not. [REDACTED] stated that he had a co-worker of his search for CLINTON's name within their platform. In order to protect the FBI's inquiry at [REDACTED] had the co-worker search for CLINTON's name in the system, along with the names of two additional current Presidential candidates. The results were negative on all three searches.

b6  
b7C

[REDACTED] was then informed that the hdr22@clintonemail.com email account was published in a NEW YORK TIMES article on March 02, 2015, and that the [REDACTED] login attempts occurred on the following day. [REDACTED] stated that this made sense to him. Given that information, he theorized that the login attempts were likely made by one of their "good guy" clients, possibly to conduct a damage assessment on the social media footprint associated with that email address. However, [REDACTED] stated that he could not verify his theory, as [REDACTED] had no additional data to corroborate it.

b6  
b7C

[REDACTED] is amenable to future contact with the FBI.

b6  
b7C

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 04/14/2016

[redacted], Chief Executive Officer (CEO), [redacted] was interviewed at his place of employment, [redacted] telephone number is [redacted] and his email address is [redacted]. Also present for this interview was FBI SA [redacted] was advised that the nature of the interview was to determine whether or not [redacted] had performed any penetration testing on the clintonemail.com domain. After being advised of the identity of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b6  
b7c

[redacted] did not perform any penetration testing for the clintonemail.com domain. [redacted] recalled that the clintonemail.com domain was previously hosted at the PLATTE RIVER NETWORKS (PRN) Internet service provider in Denver, Colorado. [redacted] is good friends with [redacted] who is [redacted] at PRN. [redacted] recalled speaking with [redacted] about doing penetration testing on that domain, approximately six months prior the large media coverage of the private server. [redacted] provided security recommendations for the system; however, actual penetration testing did not ultimately occur.

b6  
b7c

[redacted] maintains a working business relationship with PRN. If a PRN customer wishes to have penetration testing performed on their network, PRN will then refer that customer to [redacted]. Correspondingly, [redacted] will refer their customers to PRN, if they wish to harden their network systems subsequent to a [redacted] penetration testing assessment. [redacted] also leverages technical resources at PRN for other projects, including incident handling and forensic analysis. The two companies compensate one another with commission checks.

b6  
b7c

Investigation on 04/12/2016 at [redacted] Colorado

b6  
b7c

File # [redacted] CYBER - 26 Date dictated N/A

b3  
b7E

By SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7c

[REDACTED] recalled sharing several emails with PRN employees regarding the clintonemail.com domain. [REDACTED] primarily dealt with [REDACTED] but remembered that there were a couple of other PRN employees included on the exchanges. [REDACTED] then went to his office and printed out several email between him and [REDACTED]. Those printouts are enclosed for the file in a physical 1A envelope.

b6  
b7C

[REDACTED] never had access to the clintonemail.com domain, nor do they host any of their company services on PRN networks. The extent of [REDACTED] interactions with PRN employees, related penetration testing, and the clintonemail.com domain are documented in the email exchanges that [REDACTED] provided during this interview.

b6  
b7C

While reviewing the emails provided by [REDACTED] SA [REDACTED] identified one which references a public news article, where an individual named [REDACTED] had utilized a scanning tool called FIERCE to identify the addresses used for HILLARY CLINTON's (CLINTON's) personal email server. [REDACTED] provided that the referenced [REDACTED] provided that [REDACTED] formerly managed an Internet blog where he posted new hacks and exploits on almost a daily basis. A few years ago, however, [REDACTED] went dark and discontinued publishing his findings on the Internet. [REDACTED] provided that [REDACTED] goes by the name of [REDACTED] within the hacking community.

b6  
b7C

[REDACTED] has known [REDACTED] for several years. The two of them share a passion for music. [REDACTED] recalled that [REDACTED] a business that put on large-scale rock concerts, which would rival that of a Madonna-sized concert. [REDACTED] the two share music as a common bond. Additionally [REDACTED] recalled that [REDACTED] a blimp company that provided aerial coverage over large public events.

b6  
b7C

[REDACTED] recalled meeting [REDACTED] at a Colorado technical event, which [REDACTED] referred to the event as a leads event, which was a technical expo in Colorado where information technology experts could exchange ideas and network with one another. During that event, [REDACTED] spoke on a panel with [REDACTED] and a US SECRET SERVICE Agent, named [REDACTED]. During introductions with one another prior to the event, [REDACTED] recalled USSS SA [REDACTED] stating to [REDACTED] that he had recently served a warrant at PRN. [REDACTED] surmised that statement to relate to the on-going investigation of CLINTON's email server. Agent Note: A follow-up call to USSS SA [REDACTED] identified

b6  
b7C

warrant referenced in that conversation was served in support of different matter.

[REDACTED] views [REDACTED] as a "good guy", who is caught in a bad situation. [REDACTED] has stated his frustrations to [REDACTED] regarding the CLINTON email investigation. [REDACTED] stated that it has had a direct impact on PRN's business, and that they have spent a large amount of money in legal fees related to the matter. Primarily, [REDACTED] is concerned over the negative publicity that PRN has received in the news media. Additionally, PRN has been asked to step out of certain requests for proposals (RFP's) as a result of the investigation.

b6  
b7C

In addition to [REDACTED], [REDACTED] has also had limited interactions with PRN's [REDACTED] Last Name Unknown (LNU). However, [REDACTED] has been [REDACTED] primary point of contact at PRN.

b6  
b7C

When asked whether or not [REDACTED] utilizes the [REDACTED] social media cyber security product, [REDACTED] stated that they do not.

b6  
b7C

[REDACTED] is amenable to future contact with the FBI.

b6  
b7C

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 11/24/2015

[redacted] date of birth (DOB) [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and [redacted] at the law offices of DAY PITNEY located at One Canterbury Green, Stamford, CT 06901. Also present for the interview were DAY PITNEY attorneys [redacted] and [redacted]. After being advised of the identity of the interviewing Agents, and the nature of the interview, [redacted] provided the following information:

b6  
b7C

[redacted] is currently employed as [redacted] at DATTO located at 101 Merritt 7, Norwalk, CT 06851, and has held that position for [redacted]. Prior to that, [redacted] was [redacted] and worked partly as the [redacted] to DATTO.

b6  
b7C

DATTO is a company that provides products and services to small businesses related to cloud storage and disaster recovery. DATTO had an established relationship with PLATTE RIVER NETWORKS (PRN) and provided them server back-up and recovery services for some time. DATTO's relationship with PRN was already established in 2013 when PRN acquired a new contract to manage an email server with a client known to DATTO as CESC. At the time, DATTO did not know who PRN's client CESC was.

When PRN reached out to DATTO in May 2013 to provide back-up services for the CESC client server, PRN requested a slightly different service from DATTO than they normally request. Typically, PRN would request that DATTO back-up remotely to DATTO's secure cloud. For the CESC client server, PRN requested that the server be backed-up

Investigation on 11/19/2015 at Stamford, CT

File # [redacted] 302 - 37 Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted] 12/4/15

b6  
b7C



Continuation of FD-302 of Interview of [REDACTED] , On 09/02/2015 , Page 2b6  
b7C

locally and privately. At the time of this request, it was not only a new request for PRN, but a non-standard process for DATTO. In order to affect the private, local storage needs for PRN's CESC client, PRN ordered a SIRIS 2000 device from DATTO, but forgot, or did not know, to also order the private node that the data would be routed to and stored on. Because of this, the default on the DATTO configured SIRIS 2000 sent the CESC server back-up data remotely to DATTO's secure cloud and not to a local private node. This default configuration on the SIRIS 2000 has since been changed.

[REDACTED] stated that PRN must have known data was being logged in DATTO's secure cloud and not on a local private node. As evidence, [REDACTED] stated the partner portal, that PRN had log-in credentials to, had a feature displaying backed-up data and options to delete cloud or delete local. [REDACTED] stated PRN would have seen their back-ups under delete cloud. Additionally, [REDACTED] was shown a document provided by DATTO indicating email records were manually deleted from the DATTO secure cloud back-ups of the PRN CESC server in March 2015. [REDACTED] stated that it couldn't have been a DATTO employee that deleted those email records, because there would have been a work ticket indicating as much. Concerning the IP addresses associated with the March 2015 deletions, [REDACTED] thought [REDACTED] was the DATTO relay server handling the connection and [REDACTED] was a local host connection. [REDACTED] stated PRN had log-in credentials on the partner portal that weren't tied to one employee, so he did not know who from PRN logged in at any given time.

b6  
b7C

b4

Data is sent to the DATTO cloud through Secure File Transfer Protocol (SFTP) from the local DATTO device purchased by the client. Multiple DATTO devices, for different clients, are synced to one node for unified data storage. Each DATTO device is segmented on that node and only writes to a directory paired with the corresponding device. The data on the servers is partially encrypted and a password would be needed to access remotely.

The DATTO server farm is housed in Pennsylvania, multiple levels underground, in a secure facility. In order to access the facility, you must be a client there and process through security, which includes a biometrics scan. The cages that house the servers are also locked.

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 09/02/2015, Page 3

b6  
b7C

DATTO virtualizes systems locally on the DATTO appliance or remotely in the DATTO secure cloud. As part of this process, an automatic test is conducted to verify the virtualization where screenshots of the windows login screen are sent to DATTO clients. Many of DATTO's clients, to include PRN, would occasionally get "backup verification failure" notices showing their DATTO device was unbootable. \_\_\_\_\_ indicated this notice occurred very frequently and almost always was an issue involving the virtual environment and not DATTO actually failing to maintain back-ups of the associated servers. This issue was usually resolved with a handful of solutions to include changing drivers and controllers or lengthening windows for verification.

b6  
b7C

DATTO never altered or configured the retention settings regarding the period of time or frequency that the PRN server was backed up. The retention settings are set by the client.

On 08/13/2015, after the CESC client was known to DATTO and lawyers became involved regarding the retention, preservation and production of records regarding the CESC client, DATTO shipped a new SIRIS 2000 device to PRN. The impetus to the shipment was the realization that the SIRIS device originally purchased by PRN was not encrypted. The provision of the new SIRIS device was initiated by DATTO and brokered by their attorney, \_\_\_\_\_. DATTO provided the device to have increased security while also ensuring continuity of operation on the server.

b6  
b7C

\_\_\_\_\_ stated the DATTO secure cloud is frequently scanned and he has no knowledge of any intrusion or deep penetration of their systems. \_\_\_\_\_ stated the best place to look for network intrusion is the system logs.

b6  
b7C

\_\_\_\_\_ never discussed federal records retention or classified information with any representative of PRN or CESC.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/30/2015

[redacted] Records Management Division, Records Information and Dissemination Section, Winchester, Virginia was interviewed at FBI Headquarters, Washington, D.C. After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

[redacted] resides at [redacted] telephone [redacted] has been employed in the Records Management Division for the past [redacted] years.

Approximately 6 weeks ago, [redacted] received an email from [redacted] of the Department of State (STATE) Freedom of Information Act (FOIA) section. [redacted] email enclosed copies of 5 email communications from former Secretary of State HILLARY CLINTON's private email account which STATE believed may contain "FBI equities." STATE requested the FBI conduct an appropriate classification review of the emails prior to their scheduled FOIA public release. [redacted] advised these 5 emails were transmitted to him on a classified email system but were marked unclassified. [redacted] recognized that at least 1 of the emails appeared classified and forwarded same to the Counterterrorism Division (CTD) for classification review. These emails were reviewed by [redacted] and [redacted] of CTD. [redacted]

[redacted] relayed these findings to STATE as per protocol.

Approximately 1 week later, STATE's Office of Legal Counsel (OLC) contacted [redacted] and questioned the FBI's SECRET//NOFORN determination. [redacted] could not recall the name of the caller. According to OLC, [redacted] does not have an official government and therefore it believed the FBI could not classify a document based on the FGI caveat. OLC also advised that they, not the FBI, are the judge of potential harm to foreign governments and therefore the FBI did not have the right to classify a document based on those conditions. [redacted]

[redacted] as such remained classified at the SECRET//NOFORN level. [redacted] firmly

Investigation on 07/30/2015 at Washington, D.C.

File # [redacted] Date dictated N/A

By SA [redacted] SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7cb6  
b7cb6  
b7cb3  
b6  
b7cb6  
b7c

b3

b3  
b6  
b7cb3  
b7Eb6  
b7cb6  
b7c

Continuation of FD-302 of [redacted] Interview of [redacted] On 07/30/2015, Page 2  
believed, based on his position as an Original Classification Authority (OCA), that the email was classified properly and accurately.

b6  
b7c

Shortly thereafter, [redacted] received a call from [redacted] of the International Operations Division (IOD) of the FBI, who "pressured" him to change the classified email to unclassified. [redacted] indicated he had been contacted by PATRICK KENNEDY, Undersecretary of State, who had asked his assistance in altering the email's classification in exchange for a "quid pro quo." [redacted] advised that, in exchange for marking the email unclassified, STATE would reciprocate by allowing the FBI to place more Agents in countries where they are presently forbidden.

b6  
b7c

Following the above exchange, [redacted] was summoned to an "all agency" meeting at STATE to discuss matters pertaining to the classification review of pending CLINTON FOIA materials. [redacted] official from STATE, along with representatives from CIA, DIA and other government agencies were present. PATRICK KENNEDY presided over the meeting. During the conversation, a participant specifically asked whether any of the emails in question were classified. Making eye contact with [redacted] KENNEDY remarked, "Well, we'll see." [redacted] believed this was reference to the FBI's categorization of the SECRET//NOFORN email which KENNEDY was attempting to influence. In a private meeting with KENNEDY following the all agency meeting, KENNEDY asked [redacted] whether the FBI could "see their way to marking the email unclassified?" According to [redacted] KENNEDY spent the next 15 minutes debating the classification of the email and attempting to influence the FBI to change its markings. Since [redacted] continued to assert that the email was appropriately marked SECRET//NOFORN, KENNEDY asked who else in the FBI he could speak with on the matter. [redacted] referred KENNEDY to MICHAEL STEINBACH, Assistant Director of CTD.

b6  
b7c

[redacted] was then present during a conference call involving KENNEDY and STEINBACH in which KENNEDY continued to pressure the FBI to change the classified markings on the email to unclassified. STEINBACH refused to do so. Prior to ending the conversation, KENNEDY asked whether the FBI or STATE would conduct the public statements on the matter. STEINBACH advised KENNEDY that the FBI would not comment publicly on the matter. The conference call ended and, according to [redacted] the Associated Press (AP) published the story within the hour. Former Secretary of State CLINTON appeared in front of the press

b6  
b7c

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 07/30/2015, Page 3  
shortly thereafter to deny having sent classified emails on her  
private email server.

b6  
b7C

\_\_\_\_\_ believes STATE has an agenda which involves minimizing the  
classified nature of the CLINTON emails in order to protect STATE  
interests and those of CLINTON. Since the above incidents, \_\_\_\_\_ has  
received approximately 8 or 9 more emails from STATE involving FBI  
equities, 1 of which he believes may be classified SECRET//NOFORN.

b6  
b7C

UNCLASSIFIED//~~FOUO~~ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-05-2016 BY J37J85T94 NSICG

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/03/2015

(U//~~FOUO~~) [redacted] Federal Bureau of Investigation (FBI) [redacted] International Operations Division (IOD), who is currently [redacted] retirement on [redacted] was interviewed in person by FBI Special Agents [redacted] and Supervisory Special Agent (SSA) [redacted] at a [redacted] located at [redacted]. After being advised of the identity of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) As [redacted] interacted with PATRICK F. KENNEDY, U.S. Department of State (DoS) Under Secretary of State for Management, [redacted] and KENNEDY's relationship was professional. The two got along, but did not agree on many matters related to the FBI's role and authority overseas.

b6  
b7C

(U//~~FOUO~~) In late May or early June, [redacted] found a note on his desk indicating KENNEDY contacted him. [redacted] was surprised, as both his Assistant Director (AD) JOHN BOLES and Executive Assistant Director (EAD) ROBERT ANDERSON, had both been trying to contact KENNEDY for months without response.

b6  
b7C

(U//~~FOUO~~) When [redacted] returned KENNEDY's call, KENNEDY asked [redacted] assistance in changing a classification of FBI information contained in an e-mail. KENNEDY did not provide [redacted] with the e-mail, however, he told [redacted] that [redacted] of FBI's Records Management Division (RMD) [redacted] was the one that told KENNEDY the document was classified.

b6  
b7C

(U//~~FOUO~~) KENNEDY told [redacted] that the FBI's classification of the e-mail in question caused problems for KENNEDY and KENNEDY wanted to classify the document as "B9." KENNEDY further stated that the "B9" classification would allow him to archive the document in the basement of DoS never to be seen again. [redacted] was not sure of what KENNEDY meant by a "B9" classification [Note: B9 may be a reference to a FOIA exemption].

b6  
b7C

(U//~~FOUO~~) Not yet knowing the e-mail's content, [redacted] told KENNEDY he would look into the e-mail matter if KENNEDY would provide authority concerning the FBI's request to increase its personnel in Iraq.

b6  
b7C

Investigation on 09/03/2015 at Washington, DC

b3  
b7E

File # [redacted] 302 - 2 Date dictated N/A

By SSA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UNCLASSIFIED//~~FOUO~~

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 08/05/2015, Page 2

b6  
b7C

(U//~~FOUO~~) Following his conversation with KENNEDY, \_\_\_\_\_ contacted \_\_\_\_\_ to discuss the e-mail of concern. \_\_\_\_\_ told \_\_\_\_\_ the e-mail of KENNEDY's concern was classified by the FBI Counterterrorism Division (CTD) and was related to the attacks on the U.S. Consulate in Benghazi. Following his conversation with \_\_\_\_\_ contacted KENNEDY and informed him that there was no way he could assist KENNEDY with declassifying the information contained in the e-mail.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ told ANDERSON and BOLES about KENNEDY's request to declassify the e-mail and \_\_\_\_\_ response denying the ability to do so, however, \_\_\_\_\_ did not discuss the content of the e-mail with them.

b6  
b7C

(U//~~FOUO~~) Agent notes are maintained in a 1A envelope.

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 1/19/2016

(U//FOUO) On December 16, 2015, [redacted] Owner and Chief Technology Officer [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted]. Also present for the interview was [redacted] attorney, [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

(U//FOUO) [redacted] founded [redacted] while living in Chicago and currently has a family of approximately [redacted] employees comprised of full and part-time employees, as well as subcontractors. In early 2013, [redacted] a business associate of [redacted] contacted her about a client who needed a new email server. After [redacted] expressed an interest in the project and understood the clients were HILLARY AND WILLIAM CLINTON, [redacted] put her in contact with CHERYL MILLS. A few other [redacted] personnel assisted with invoicing and technical aspects of the contract, but [redacted] did most of the work herself. [redacted] primary contacts were MILLS and BRYAN PAGLIANO; MILLS helped produce the proposal and PAGLIANO assisted in developing the requirements for the server architecture. [redacted] started the discussion by providing a range of options from low-cost Gmail to a more sophisticated private server. She understood the client's impetus for the project to be reliability/uptime and security in the wake of a situation where the client's private server housed in their residence experienced one week of downtime because of a storm. The client selected the private server from the options provided by [redacted]. Backup systems were planned for Phase 2 of the project, but [redacted] was not involved in those decisions.

b6  
b7C

(U//FOUO) As part of the initial conversations with PAGLIANO and MILLS [redacted] knew at one point the domains and number of email accounts on the server, but could not recall those details. Additionally [redacted] had no knowledge of email servers owned or operated by the client prior to the equipment maintained by PAGLIANO.

b6  
b7C

(U//FOUO) After the client selected a private server [redacted] contacted two firms she had prior experience with: GRAVITAS, a large Information Technology firm, and PLATTE RIVER NETWORKS (PRN), a small boutique firm. After the client selected PRN, [redacted] worked with MILLS, PAGLIANO, and [redacted] to develop the details of the project. [redacted] was only involved in one or two meetings; [redacted] believed he was curious about the process. PAGLIANO handled the technical aspects of the project and MILLS handled strategic concerns. As PRN took over day-to-day management, [redacted] involvement gradually faded out. The client occasionally reached out for assistance and [redacted] would help where she could. Payment for her services was billed for the entire task, not hourly, so she did not charge any fee for this assistance.

b6  
b7CInvestigation on 12/16/2015 at New York, NYFile # [redacted] 302 - 49 Date dictated N/Ab3  
b7EBy SA [redacted] 1/19/2016b6  
b7C



Continuation of FD-302 of Interview of [REDACTED], On 12/16/2015, Page 2b6  
b7C

(U//~~FOUO~~) [REDACTED] believed a CloudJacket-type security device was part of the project design, so when it wasn't part of the initial install, she pushed for the implementation of it after the migration from the PAGLIANO server to the PRN server. During the migration, she was not in the weeds, but knew enough to know it was done correctly from a security standpoint. [REDACTED] was not aware of any security intrusions or compromises while she was involved in the day-to-day operations of the transition, nor was she brought back in after the fact on any security issues. In addition to the CloudJacket, as part of the security considerations, [REDACTED] discussed transitioning from BlackBerries to the iPhone with the client, as well as blocking international access to the server. Ultimately, the client chose to stay with BlackBerries and international blocking was declined because the client frequently traveled internationally.

b6  
b7C

(U//~~FOUO~~) Since press reports of [REDACTED] association with PRN and the CLINTON's went public, [REDACTED] and some partners contracted Depth Security to conduct Vulnerability Threat Assessments for some of their shared clients. [REDACTED] was not aware of any such assessment conducted on the CLINTON's server.

b6  
b7C

(U//~~FOUO~~) [REDACTED] had no knowledge of the following topics as they relate to the PAGLIANO or PRN servers:

b6  
b7C

- moving emails to a new domain
- laptop backups
- temporary backups
- classified information
- federal records

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/26/2016

(U//~~FOUO~~) On May 23, 2016, [redacted] date of birth [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and SA [redacted] at the offices of Platte River Networks (PRN) located at 5700 Washington Street, Denver, Colorado 80216. Also present for the interview was [redacted] and via speaker phone, [redacted] both attorneys at the [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] was given PRN administrator credentials to the Clinton Executive Service Corporation (CESC) email server, but could not recall logging in to the server. [redacted] understood [redacted] [redacted] were in charge of handling the CESC client [redacted] recalled he assisted with the CESC client less than five times. He recalled he once assisted someone from CESC in updating their operating system. [redacted] talked to [redacted] Last Name Unknown (LNU) from CESC most times.

b6  
b7C

(U//~~FOUO~~) [redacted] was not aware of a laptop containing an archive of email belonging to HILLARY CLINTON that was shipped to PRN around February 2014. [redacted] was not aware what became of the foregoing laptop.

b6  
b7C

(U//~~FOUO~~) [redacted] was not aware of any support PRN provided the CESC client from October 2014 to January 2015. [redacted] was not aware of any CESC request to delete, wipe or shred their email records. [redacted] was not aware of any email content being transmitted to CESC.

b6  
b7C

(U//~~FOUO~~) At this point in the interview, Agents displayed PRN provided records and email from the March 2015 timeframe. [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] was not aware of a trip made by PRN employee [redacted] to the Equinix data center in Secaucus, New Jersey.

b6  
b7C

(U//~~FOUO~~) After Agents displayed an email dated March 09, 2015 where CHERYL MILLS discussed preservation of materials, [redacted] had no knowledge of the email or any request by any entity to preserve CESC related data.

b6  
b7C

Investigation on 05/23/2016 at Denver, Colorado

File # [redacted] 302 - 99 Date dictated N/A

b3  
b7E

By SA [redacted]

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 07/23/2015, Page 2

(U//~~FOUO~~) \_\_\_\_\_ has no recollection of a conference call on March 25, 2015 or March 31, 2015 with CESC. \_\_\_\_\_ stated CESC never requested their email content be deleted, wiped or shredded.

(U//~~FOUO~~) \_\_\_\_\_ was unaware of any PRN employee conducting manual deletions of the DATTO device used to back-up the CESC email server.

(U//~~FOUO~~) \_\_\_\_\_ was unaware of any successful computer intrusion of the CESC server.

(U//~~FOUO~~) Notes of the interview and documents displayed to \_\_\_\_\_ will be maintained in a FD340 envelope and filed with the captioned investigation.

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/29/2016

(U//FOUO) On June 29, 2016 [redacted] Assistant to President William J. Clinton, [redacted] was interviewed telephonically by Federal Bureau of Investigation (FBI) Special Agents [redacted] Representing [redacted] and also present for the call, was [redacted] from The Department of Justice (DoJ) Counterintelligence and Export Control Section also participated in the call. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] was not familiar with Tor, which enables anonymous communication, nor did [redacted] ever use Tor. [redacted] described herself as a "very low tech person."

b6  
b7C

(U//FOUO) [redacted] used various communication devices and computer to remotely sign into her @presidentclinton.com email account. These devices included an iPhone, BlackBerry, and on rare occasions, a laptop. [redacted] also accessed her @presidentclinton.com email account from her desktop computer at the Clinton Foundation. [redacted]s desktop computer operated off of Windows, but she was not sure of the specific version. [redacted] further stated that she used an Apple Mac on occasion to sign onto her email.

b6  
b7C

(U//FOUO) [redacted] did not recall experiencing any unusual spam or phishing email activity related to her @presidentclinton.com email account in January, 2013. [redacted] was in New York on January 5, 2013.

b6  
b7C

(U//FOUO) A copy of the original interview notes are attached in a 1A envelope.

Investigation on 6/29/2016 at Washington, D.C.b3  
b7EFile # [redacted]-302 -88 Date dictated N/ABy SA [redacted]SA [redacted]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 09/21/2015

On September 14, 2015, [redacted] Platte River Networks, date of birth [redacted] social security number [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted]. Also present for the interview was [redacted] from [redacted] and Department of Justice (DOJ) Attorney [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following:

b6  
b7C

In February or March 2013, [redacted] was informed by [redacted] at Platte River Networks (PRN), of a potential contract managing email for a high profile client, but did not know who the client was. [redacted] was not involved in the proposal or technical solution for the client, nor did he have any first hand meetings with anyone representing the client. [redacted] and [redacted] handled those matters. [redacted] eventually learned the client was WILLIAM CLINTON and HILLARY CLINTON (CLINTON), doing business through a company named CESC. At some point during the process, CESC conducted background checks on the individuals who would provide the technical support for the contract. Those individuals were [redacted] and [redacted] did not know why CESC conducted the background checks, but assumed it was because they were a high profile client.

b6  
b7C

On or about March 2015, [redacted] first learned about concerns regarding CLINTON's use of a private email server when it was reported by the media. Due to this increased attention, PRN decided to place Internet Protocol (IP) country blocks and took other additional steps to secure the CESC server. In the same timeframe, [redacted] participated in a conference call with CLINTON's counsel, Williams and Connolly, to determine where CLINTON's email was stored. While [redacted] was on the call, [redacted] and [redacted] handled most of the questions. Subsequently, PRN received a preservation letter from the United States Senate and a preservation request from the FBI. PRN brought their own counsel on board to assist with these requests.

b6  
b7C

After receiving the FBI's preservation request, PRN received a letter from Williams and Connolly instructing them to give the FBI the CESC server used prior to migrating email to PRN acquired equipment. [redacted] traveled to New Jersey and turned over the server to the FBI. [redacted] stated [redacted] did not power up the server before providing it to the FBI.

b6  
b7C

The CESC email server architecture also involved a DATTO backup appliance. The DATTO was configured to store backup data locally, however, due to a glitch, DATTO backed up data to their cloud for a period of time. On or about August 24, 2015, DATTO sent PRN a letter stating they would stop

Investigation on 09/14/2015 at Denver, Colorado

File # [redacted] 302 -13 Date dictated N/A

b3  
b7E

By SA [redacted]

SA [redacted]

10/1/2015

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 09/14/2015, Page 2

b6  
b7C

backing up to their cloud and preserve what was in their possession. The DATTO has a 60 day purge cycle, therefore, DATTO should have data from 60 days prior to August 24, 2015.

\_\_\_\_\_ stated \_\_\_\_\_ and \_\_\_\_\_ would have specific details regarding the CESC email server project. \_\_\_\_\_ never heard anyone related to the CESC project discuss the existence of classified information on the server.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/26/2016

(U//FOUO) On May 23, 2016, [redacted] date of birth [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and SA [redacted] at the offices of Platte River Networks (PRN) located at 5700 Washington Street, Denver, Colorado 80216. Also present for the interview was [redacted] and via speaker phone, [redacted] both attorneys at the [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] was not aware of a laptop containing an archive of email belonging to HILLARY CLINTON that was shipped to PRN around February 2014. [redacted] was not aware what became of the foregoing laptop.

b6  
b7C

(U//FOUO) [redacted] only recently was made aware of a CLINTON email archive file being transmitted to the Clinton Executive Services Corporation (CESC) around July 2014 and September 2014 by [redacted] was not aware of the request by CESC, or transmittal by [redacted] as it was occurring [redacted] was not aware of what specifically was requested by CESC or exactly how [redacted] fulfilled the request [redacted] never spoke with anyone at CESC.

b6  
b7C

(U//FOUO) [redacted] was not aware of any support PRN provided the CESC client from October 2014 to January 2015 [redacted] was not aware of any CESC request to delete, wipe or shred their email records.

b6  
b7C

(U//FOUO) At this point in the interview, Agents displayed PRN provided records and email from the March 2015 timeframe. [redacted] provided the following information:

b6  
b7C

(U//FOUO) In March 2015, when various media outlets reported a private email domain and server was used by HILLARY CLINTON, PRN decided to create an internal "share drive" and control access to only the PRN employees working the CESC account. PRN never deleted information pertaining to the CESC client and provided the FBI all records they maintained pertaining to CESC.

(U//FOUO) In March 2015, [redacted] stated PRN employee [redacted] travelled to the Equinix data center to check the security of the servers and to ensure they were "locked tight." After the media reports, PRN was even more concerned about the security of the server.

b6  
b7C

Investigation on 05/23/2016 at Denver, Colorado

File # [redacted] 302 - 96 Date dictated N/A

b3  
b7E

By SA [redacted]

SA [redacted]

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 07/23/2015, Page 2

(U//~~FOUO~~) After Agents displayed an email dated March 09, 2015 where CHERYL MILLS discussed preservation of materials, [REDACTED] could not recall any other request by any entity to preserve CESC related data. [REDACTED] received guidance from PRN attorneys and understood CESC client information and records should not be destroyed. [REDACTED] believed the preservation request applied more to CESC records and not necessarily email content. [REDACTED] believed the preservation request to be a request from the government.

b6  
b7C

(U//~~FOUO~~) [REDACTED] had no specific recollection of a conference call on March 25, 2015 or March 31, 2015 with CESC. [REDACTED] stated CESC never requested their email content be deleted, wiped or shredded. [REDACTED] had a memory of a request by CESC to confirm their server back-ups were still working, but could not recall the specific request. [REDACTED] was aware CESC wanted their email retention policy changed to 60 days.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was unaware of any successful computer intrusion of the CESC server.

b6  
b7C

(U//~~FOUO~~) Notes of the interview and documents displayed to [REDACTED] will be maintained in a FD340 envelope and filed with the captioned investigation.

b6  
b7C



ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED

DATE 10-13-2016 BY J37J85T94 NSICG **FEDERAL BUREAU OF INVESTIGATION**

Date of transcription 08/17/2015

On August 17, 2015, KATHERINE M. TURNER, Partner at the law offices of Williams & Connolly LLP, 725 12<sup>th</sup> Street, N.W. Washington, D.C. met at her place of employment with Agents of the FBI to discuss voluntarily turning over six (6) laptop computers in her possession known to contain Top Secret classified information. Also in attendance were [redacted] of the FBI's Office of General Counsel, [redacted] Trial Attorney for the Counterespionage Section at the Department of Justice, [redacted] an attorney with Williams & Connolly LLP, and [redacted] counsel for CHERYL MILLS, from the law offices of Paul, Weiss, Rifkind, Wharton & Garrison LLP.

b6  
b7C

Prior arrangements had been made to meet at this time and place to discuss an agreement through which Williams & Connolly would voluntarily turn over to the FBI six (6) laptops computers used by the firm to view email communications from the private server of former Secretary of State HILLARY CLINTON. TURNER acknowledged that these laptops contain Top Secret email communications and attorney/client privileged communications. TURNER sought to turn over the laptops as soon as possible but wished to ensure that privileged communications on the laptops would remain confidential. TURNER declined to provide consent to search the laptops and wished to arrange for secure storage of them in a manner agreeable to both the FBI and the attorneys. The FBI agreed to provide TURNER with a draft letter outlining the proposed conditions of storage as soon as possible.

Contrary to statements made on August 6, 2015, TURNER advised that only five of the six laptops are in the possession of Williams & Connolly, the sixth being in the possession of [redacted] counsel for CHERYL MILLS, former Chief of Staff for CLINTON. [redacted] admitted that the computer in his possession has been connected to the Internet on numerous occasions subsequent to being loaded with the classified email communications of HILLARY CLINTON. This laptop was possessed by CHERYL MILLS but utilized by HEATHER SAMUELSON, an attorney on her staff, to conduct a review of approximately 60,000 emails originally contained on CLINTON's private email server. According to [redacted] SAMUELSON deleted CLINTON's personal emails

b6  
b7C

Investigation on 08/17/2015 at Washington, D.C.

b3  
b7E

File # [redacted]-81 Date dictated N/A

By SA [redacted]

b6  
b7C

Continuation of FD-302 of Interview of Katherine M. Turner, On 08/6/2015, Page 2  
from the original 60,000 resulting in the 30,490 emails eventually  
turned over to the FBI. [ ] claimed the other emails had been  
deleted from the laptop but was unable to specify whether they had  
been forensically wiped to an unrecoverable state.

b6  
b7C

Both [ ] and TURNER admitted that the emails contained on  
these laptops had been viewed by attorneys who did not have a security  
clearance at the time they reviewed the material. TURNER said the  
emails did not contain classification markers and thus they were not  
aware that they were classified at the time.

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-13-2016 BY J37085T94 NSICG

Date of transcription 12/11/2015

(U//~~FOUO~~) On December 10, 2015 [redacted] date of birth [redacted] of the Office of the Legal Adviser, Financial Disclosure Division, U.S. Department of State was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted]. Also present were [redacted] Trial Attorney, Public Integrity Section, U.S. Department of Justice and [redacted] Attorney Adviser, U.S. Department of State. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) In 2009 [redacted] worked as an Ethics Analyst for the U.S. Department of State. She was responsible for reviewing the Financial Disclosure Forms (SF-278) of new and current employees to assess if their investments, or outside income sources, created a conflict of interest with their position at the U.S. Department of State. When [redacted] had questions about the filer's SF-278 she would contact them directly, either telephonically or via email, to clarify the filer's responses. [redacted] would then amend the SF-278 to reflect any corrections or clarifying information provided by the filer. She would then send a copy of the updated SF-278 to the filer for their personal records. Once the SF-278 was finalized an assessment was made on whether the filer's investments, or other financial interests, posed a potential conflict of interest. The assessment was then signed off on by [redacted] supervisor, [redacted]. Upon completing the review a physical file containing the SF-278 and supporting documents were maintained for a finite period of time before it was destroyed.

b6  
b7C

(U//~~FOUO~~) [redacted] was shown copies of the following documents:

b6  
b7C

- New Entrant SF-278 submitted by BRYAN PAGLIANO on April 15, 2009
- Email from [redacted] to PAGLIANO dated August 25, 2009, with the subject "Ethics Clearance... (Reply Requested)"
- New Entrant SF-278 submitted by BRYAN PAGLIANO on April 15, 2009, with handwritten updates
- Incumbent SF-278 submitted by PAGLIANO on April 4, 2010

b6  
b7C

(U//~~FOUO~~) After reviewing the documents, [redacted] confirmed that she had sent the above referenced email to PAGLIANO to clarify some of his responses on his original SF-278. [redacted] provided that the email contained her original message to PAGLIANO and did not appear to have been

b6  
b7C

Investigation on 12/11/2015 at Washington, D.C.

b3  
b7E

File # [redacted] 302 - 39 Date dictated N/A

By SA [redacted]

b6  
b7C

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 12/11/2015, Page 2

altered in any way. \_\_\_\_\_ also confirmed that it was her handwriting on the updated New Entrant SF-278 form and that the handwritten notes reflected additional information provided by PAGLIANO in response to her email. \_\_\_\_\_ could not recall any additional information about her exchange with PAGLIANO, aside from what she had written on the updated SF-278. \_\_\_\_\_ believed that PAGLIANO had provided the updated information to her via email but she no longer had those emails because she purged her emails when she changed positions at the U.S. Department of State. \_\_\_\_\_ further noted that the physical file could not be found and had likely been destroyed.

b6  
b7C

(U//FOUO) \_\_\_\_\_ reviewed the Incumbent SF-278 form filed by PAGLIANO and noted that she did not conduct the review of that document. \_\_\_\_\_ pointed out the checkmarks on the form and stated that they were not her handwriting. \_\_\_\_\_ did not know who reviewed the form but stated that \_\_\_\_\_ should be able to identify the reviewer based on internal computer records.

b6  
b7C

(U//FOUO) With respect to the Incumbent SF-278 form filed for 2009, \_\_\_\_\_ stated that all income and compensation from 2009 should have been captured in Schedule A. This includes any income in the calendar year, even if it was received prior to his start date with the U.S. Government. \_\_\_\_\_ noted that the only exception to this would be if the income was from another government entity. However, income from a political action committee or another campaign related organization would not qualify as other government employment.

b6  
b7C

(U//FOUO) \_\_\_\_\_ noted that in 2009 the filer would have been provided with several pages of instructions on how to correctly and accurately complete the form. \_\_\_\_\_ provided an electronic copy of the instructions to the interviewing agents.

b6  
b7C

(U//FOUO) A copy of the above referenced documents and the original interview notes are attached in a 1A envelope.

## FEDERAL BUREAU OF INVESTIGATION

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-13-2016 BY J37J85T94 NSICG

Date of transcription 09/02/2015

On September 2, 2015, [REDACTED] a Special Agent with Homeland Security Investigations (HSI), Department of Homeland Security (DHS), Norfolk Virginia, was interviewed at the Federal Bureau of Investigation (FBI). After being advised of the identity of the interviewing Agent and the nature of the interview, [REDACTED] provided the following information:

b6  
b7C

[REDACTED] was previously an agent with the U.S. Department of State, Bureau of Diplomatic Security (DS). [REDACTED] left DS in approximately [REDACTED] spouse, [REDACTED] was also a prior DS agent who, from 2007-2009, served as an Assistant Shift Leader on former Secretary of State CONDOLEEZZA RICE's and HILLARY CLINTON's protective details. [REDACTED] served briefly on former Secretary CLINTON's protective detail in 2009. From her own experience, and information obtained through [REDACTED] and other agents, [REDACTED] described a "stark difference" between RICE and CLINTON with regard to obedience to security and diplomatic protocols. RICE observed strict adherence to State Department security and diplomatic protocols while CLINTON frequently and "blatantly" disregarded them. For example, it is standard security and diplomatic protocol for the Secretary of State to ride in the armored limousine with the local U.S. ambassador when traveling in countries abroad. It is seen as diplomatic protocol for the Secretary of State to arrive at foreign diplomatic functions with the local ambassador; however, CLINTON refused to do so, instead choosing to be accompanied in the limousine by her Chief of Staff, HUMA ABEDIN. This frequently resulted in complaints by ambassadors who were insulted and embarrassed by this breach of protocol. [REDACTED] explained that CLINTON's protocol breaches were well known throughout Diplomatic Security and were "abundant."

b6  
b7C

[REDACTED] explained that ABEDIN possessed "much more power" over CLINTON's staff and schedule than other former chiefs of staff. [REDACTED] believed that ABEDIN herself was often responsible for overriding security and diplomatic protocols on behalf of CLINTON.

b6  
b7CInvestigation on 09/02/2015 at Chesapeake, VAb3  
b7EFile # [REDACTED] - 302 - 4 Date dictated N/ABy SA [REDACTED]b6  
b7C

Continuation of FD-302 of Interview of [REDACTED] On 09/02/2015 Page 2

b6  
b7C

On a trip to Jakarta, Indonesia, in early 2009, CLINTON requested to visit an area of Jakarta that presented security and safety challenges. This visit was reportedly for a photo opportunity regarding CLINTON's "clean cooking stoves" initiative. The DS advance team recommended against traveling to this area because the route could not be secured and was lined with dangerous circumstances and individuals. As such, the DS advance team recommended in writing that this excursion be stricken from the schedule but were told by DS management that it was going to happen because "she wanted it." DS agents felt this excursion into potentially hostile areas placed CLINTON, her staff, the media, and her security detail in unnecessary danger in order to conduct a photo opportunity for "her election campaign." DS agents had the perception that CLINTON was using her position as Secretary of State to campaign for President of the United States. DS agents felt CLINTON traveled with hand-picked media who would present her in favorable light in order to garner political support. It was also believed that CLINTON disregarded security and diplomatic protocols, occasionally without regard for the safety of her staff and protection detail, in order to gain favorable press.

CLINTON traveled in an armored vehicle whose passenger windows do not open. This is a design feature for the protection of the occupants. However, the driver's window does open slightly. On one occasion while traveling to Palestine, CLINTON ordered the limousine driver, believed to be [REDACTED] to open the window while in "occupied territory", referring to a dangerous area of the West Bank. [REDACTED] initially declined to respond to CLINTON's request; however, repeated demands by CLINTON forced him to open his window despite the danger to himself and the occupants.

b6  
b7C

[REDACTED] explained that security and diplomatic breaches were often communicated from the foreign post back to the Department of State via cables from the Regional Security Officer (RSO). These cables often described incidents like those described above. [REDACTED] recommended interviewing current and former RSOs from foreign posts visited by CLINTON during her tenure for more detail into these and similar events.

b6  
b7C

Early in CLINTON's tenure as Secretary of State, she and her staff were observed removing lamps and furniture from the State Department which were transported to her residence in Washington, D.C.

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 09/02/2015, Page 3

\_\_\_\_\_ does not know whether these items were ever returned to the government upon CLINTON's departure from the State Department.

b6  
b7C

Despite having her own DS security detail, CLINTON continued to utilize a Secret Service security detail while at her residence in Chappaqua, New York. DS security would meet Secret Service security at the airport in New York and turn over protection to them. This practice was unknown to DS prior to CLINTON's tenure and often presented logistical problems to both services. \_\_\_\_\_ explained that CLINTON's treatment of DS agents on her protective detail was so contemptuous that many of them sought reassignment or employment elsewhere. Prior to CLINTON's tenure, being an agent on the Secretary of State's protective detail was seen as an honor and privilege reserved for senior agents. However, by the end of CLINTON's tenure, it was staffed largely with new agents because it was difficult to find senior agents willing to work for her. \_\_\_\_\_ claimed to have had at least one conversation with Secret Service agents who experienced the same poor treatment.

b6  
b7C

Inside CLINTON's office at the Department of State there is a security checkpoint known as "Post 1." Post 1 is staffed by a uniformed DS officer and a DS agent and provides security to CLINTON's inner office. CLINTON's office is a Sensitive Compartmented Information Facility (SCIF) and Post 1 is located within that SCIF. By DS security policy, no cell phones are allowed inside the SCIF and DS agents, officers, and staff are required to leave their cell phones outside the door in secure lockers. CLINTON refused to abide to this security requirement and brought her cell phone, believed to be a Blackberry, inside the SCIF where a DS agent assigned to Post 1 was required to guard it. DS agents were indignant that they were required to follow security policy but CLINTON made herself exempt from the same regulations.

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/11/2016

(U//FOUO) On February 10, 2016, [redacted], DOB [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at the law offices of Latham & Watkins LLP, 885 3<sup>rd</sup> Ave, New York City, NY. Also present were [redacted] and [redacted] of Latham & Watkins. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] is currently a [redacted] and a [redacted] at [redacted]. He was formerly the [redacted] at the Department of Defense (DoD) from [redacted] Prior to the DoD, [redacted] was at the National Security Council (NSC) from [redacted] until [redacted]. During that time he held the positions of [redacted] from [redacted] to the Fall of [redacted] from [redacted] until early [redacted] and then [redacted].

b6  
b7C

(U//FOUO) [redacted] provided that there were typically three to five Deputy Committee (DC) meetings a week, up to four Principal Committee (PC) meetings a week, and NSC meetings with the President as needed. Additionally, there was a weekly lunch between Secretary GATES, National Security Advisory DONILON and Secretary CLINTON. [redacted] provided that [redacted] the DoS representative for DC meetings and Secretary CLINTON was the DoS representative for PC and NSC meetings.

b6  
b7C

(U//FOUO) While at the NSC, [redacted] was responsible for working with the meeting participants, to include the Department of State (DoS), to coordinate and plan for each upcoming meeting. More specifically, [redacted] would review memorandums, prepare meeting packages and control the flow of information between the agencies. These interactions occurred through both formal and informal channels. [redacted] provided that with respect to DoS matters he primarily worked with JAKE SULLIVAN and JOE MACMANUS.

b6  
b7C

(U//FOUO) Prior to each DC and PC meeting the NSC would notify the participants of the upcoming meeting and ask that they submit their meeting packages in advance so that they could be distributed as read ahead material. [redacted] stated that he routinely worked with SULLIVAN to ensure that DoS agendas, talking points, and formal documents were received in advance of each meeting. [redacted] noted that he would sometime provide relevant documents, such as ODNI assessments, to DoS.

b6  
b7C

Investigation on 2/10/2016 at New York, NY

b3  
b7E

File # [redacted] 302 - 55 Date dictated N/A

By SA [redacted]

b6  
b7C



Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 2/10/2016, Page 2

b6  
b7C

for their use as they prepared their meeting packages. \_\_\_\_\_ stated that the classification level of the packages was dependent on the content and could be unclassified, classified or a mix. Documents and meeting packages were typically transmitted between agencies via the appropriate email system, secure fax (i.e., Washfax) or courier service.

b6  
b7C

(U//~~FOUO~~) Following each meeting an NSC staffer would take notes and then prepare a Summary of Conclusions (SOC) that summarized the issue discussed, supporting and dissenting opinions, the final outcome and any necessary action items. The SOC would then be approved by the NSC executive staff before being distributed to the meeting participants.

(U//~~FOUO~~) \_\_\_\_\_ was not aware of how or where the NSC archived the SOC and related documents for a specific DC or PC meeting.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was shown several emails that were sent in preparation for an October 2009 PC meeting regarding the U.S. strategy in Pakistan. However, after reviewing the emails \_\_\_\_\_ stated that while he remembered the topic in general he could not recall the specific PC meeting in question. He noted that at that time there were numerous meeting on the subject. Similarly, \_\_\_\_\_ could not recall the details of any of the documents referenced in the emails. While \_\_\_\_\_ could not comment on the specifics of the emails he did note that the emails were representative of the communications that were exchanged between NSC and DoS as they were preparing for a PC meeting.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was shown an email that was sent in preparation for a June 2011 PC meeting. However, \_\_\_\_\_ could not recall any specifics regarding the PC meeting in question given the limited content of the email.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes and the referenced emails are attached in a 1A envelope.

~~SECRET//NOFORN~~

-1-

## FEDERAL BUREAU OF INVESTIGATION

ALL FBI INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 10-13-2016 BY 337085T94 NSICG

Date of transcription 10/26/2015

(U//FOUO) On 10/23/2015, Special Agent (SA) [redacted] Federal Bureau of Investigation (FBI), DOB [redacted] SSAN [redacted] was interviewed in person by SA [redacted] and SA [redacted] in FBI Headquarters. After being advised of the identity of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] began working for Department of State's (DoS) Diplomatic Security Service (DSS) in [redacted] where he was assigned to the DSS Los Angeles Field Office. In [redacted] [redacted] was selected for an assignment with the Secretary of State's security detail. [redacted] served on the Secretary's detail until [redacted] when he joined the FBI as an SA and attended FBI new agent training.

b6  
b7C

(U//FOUO) When [redacted] began his stint on the Secretary's detail, CONDOLEEZZA RICE, was the Secretary of State. [redacted] detail assignment carried over to HILLARY CLINTON, when she was appointed Secretary of State in 2009.

b6  
b7C

(U//FOUO) DSS covered the majority of CLINTON's protection while she was in the Washington, DC, area. However, when her husband was in town, United States Secret Service (USSS) would cover the bulk of the protection detail responsibilities when she was with her husband or in the residence.

(U//FOUO) USSS would provide security for CLINTON's 3067 Whitehaven Street NW, Washington, DC, address during the day and DSS would cover the overnight detail. [redacted] was never inside the CLINTON's Whitehaven residence, as DSS usually posted in a vehicle outside. CLINTON had a secure telephone in her Whitehaven residence and [redacted] assumed it was in a secure room.

b6  
b7C

(U//FOUO) CLINTON usually traveled to her home in Chappaqua, NY, via a US Airways shuttle from Reagan National Airport (DCA) to Westchester County Airport in White Plains, NY. USSS would handle CLINTON's security in NY, and DSS would have a small presence to maintain CLINTON's communications. [redacted] was never inside CLINTON's Chappaqua residence. [redacted] was known as the CLINTON's Chappaqua "house guy/scheduler." The security detail would often contact [redacted] to determine the Secretary's departure time.

b6  
b7C

Investigation on 10/26/2015 at Washington, DC

b3  
b7E

File # [redacted] 302 Date dictated N/A

By SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~SECRET//NOFORN~~

Continuation of FD-302 of Interview of [REDACTED], On 10/23/2015, Page 2b6  
b7C

(U//~~FOUO~~) The Secretary's security detail chain of command was as follows:

- 1 Special Agent in Charge (SAC)
- 4 Assistant Special Agents in Charge (ASAC)
- 3 Shift Leads (SSA)
- Approximately 45 SA's assigned directly to detail shifts

(U//~~FOUO~~) [REDACTED] was the SAC during CLINTON's tenure as Secretary. [REDACTED] and [REDACTED] were two ASAC's during the same time period. [REDACTED] was [REDACTED] SSA, and both [REDACTED] and [REDACTED] were shift agents assigned with [REDACTED] to CLINTON's detail. [REDACTED], [REDACTED], and [REDACTED] are all still employed with DSS (possibly in the Washington Field Office).

b6  
b7C

(U//~~FOUO~~) CLINTON's office was located on the 7<sup>th</sup> floor of DoS Headquarters. The entire Secretary's suite was a Sensitive Compartmented Information Facility (SCIF). The DSS security detachment maintained a Post directly outside the Secretary's office. The DSS space was known as Post One (1). DSS personnel were not authorized to bring their mobile phones into Post 1, as it was located within the SCIF. CLINTON did keep a mobile phone inside a desk drawer inside Post 1, but when she would remove the phone from the desk, she would take it to a non-SCIF space to make calls or use the phone.

(U//~~FOUO~~) HUMA ABEDIN and CHERYL MILLS were among CLINTON's staff members who had offices located within the 7<sup>th</sup> floor Secretary's SCIF. In addition to ABEDIN and MILLS, [REDACTED] and JAKE SULLIVAN, were part of CLINTON's main "traveling crew." MILLS did not accompany CLINTON on many overseas trips.

b6  
b7C

(U//~~FOUO~~) [REDACTED] could not recall the specifics surrounding the electronic devices used by CLINTON's executive staff, but he assumed they were BlackBerry devices. [REDACTED] did not interact with CLINTON nor MILLS via email, but sometimes he would receive a forwarded email with their accounts listed in the chain. [REDACTED] remembered receiving email chains that contained Clintonfoundation.org accounts. [REDACTED] also thought he recalled seeing emails from [REDACTED] originating from a Gmail account, however, he was not entirely sure.

b6  
b7C

(U//~~FOUO~~) In addition to the Secretary's DSS security detail, CLINTON also traveled with a team of Security Engineers who were specifically assigned to her staff. These Security Engineers would travel overseas with CLINTON for the specific purpose of setting up and maintaining her Communications while on travel. The Security Engineer Team generally set up a secure communication post inside the Embassy, or a hotel room adjacent to where the Secretary would stay. The communication post would be manned 24 hours a day.

~~SECRET//NOFORN~~

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 10/23/2015, Page 3

b6  
b7C

(S//~~FOUO~~) The team of Security Engineers would send the necessary equipment to set up the Secretary's communications via diplomatic pouches \_\_\_\_\_

b1 per DOS

\_\_\_\_\_. As it relates to the Secretary's use of Diplomatic Pouches, \_\_\_\_\_ was unaware of the process and procedures related to the preparation and transport for overseas travel.

b6  
b7C

(U//~~FOUO~~) When traveling overseas in advance of, or with, the Secretary, the Regional Security Officer (RSO) would usually provide CLINTON's security detail a letter, prior to, or on arrival. The letter provided guidance on what to expect from a security standpoint while in a particular country.

\_\_\_\_\_ was not sure if a similar letter from the RSO was provided to the Secretary and/or her executive staff.

b6  
b7C

(U//~~FOUO~~) The Secretary's security detail would "hotwash" after an overseas trip, to compare the advance team's preparation to what actually took place during the Secretary's travel. The RSO was not a part of these after action discussions. \_\_\_\_\_ believed an RSO would send a cable to the RSO assigned to the Executive Office at DoS Headquarters if there were any security issues concerning CLINTON and/or her staff.

b6  
b7C

(U//~~FOUO~~) Agent notes are maintained in a 1A envelope.

~~SECRET//NOFORN~~

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-13-2016 BY J37J85T94 NSICG

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/26/2015

[redacted]  
[redacted] United States Department of State (STATE), 515 22<sup>nd</sup> Street NW, Washington, D.C. 20037, office telephone (202) [redacted] mobile telephone (202) [redacted] email [redacted]@state.gov, date of birth [redacted] was interviewed on his mobile telephone by FBI Special Agent [redacted]. After being advised of the identity of the interviewing Agent and the nature of the interview, [redacted] provided the following information:

The Information Programs and Services (IPS), Bureau of Administration oversaw the program for Congressional inquiries and Freedom of Information Act (FOIA) requests. The House Select Committee on Benghazi requested emails to or from former Secretary of State Hillary CLINTON related to Benghazi. It was determined there were 296 emails related to the Benghazi request. After IPS officials performed their review of the 296 emails, they referred emails for classification determination to four outside agencies, specifically the: 1) FBI; 2) CIA; 3) Department of Defense (DoD); and 4) National Security Council (NSC).

IPS officials have regular points of contact (POCs) at all agencies and STATE bureaus that the IPS would send classification determination referrals to in response to Congressional or FOIA requests. The regular POCs at the agencies listed above were as follows:

- FBI: [redacted]—no contact information provided.

- CIA: [redacted]—no contact information provided; [redacted] boss was [redacted] the CIA's FOIA branch similar to STATE's

IPS team, [redacted] email was [redacted]@ucia.gov.

- DoD: [redacted] Office of the Secretary of Defense (OSD)—no contact information provided.

- NSC: [redacted] retired now, but was the POC earlier in 2015 when the Benghazi request was processed. NSC's current POC was [redacted] telephone 202 [redacted] email [redacted]

[redacted]@nsc.gov. [redacted] believed [redacted] might inform [redacted] and [redacted] Legislative Affairs, if contacted by the FBI.

Before IPS conducted their review of the Benghazi request, [redacted] Attorney, Office of the Legal Adviser performed their own, independent review of the 296 Benghazi-related emails. [redacted] review team used different POCs at other agencies to review the 296 emails for a classification determination. [redacted] did not know why: 1) [redacted] team did a review, as that was

Investigation on 08/26/2015 at Washington, DC

File # [redacted] - 79 Date dictated N/A

By SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

b6  
b7C

b6  
b7C

b3  
b7E

b6  
b7C

b6  
b7C

Continuation of FD-302 of [redacted] interview of [redacted], On 08/26/2013, Page 2  
IPS' purview; 2) why [redacted] team used different POCs than the regular POCs IPS used; 3) what review criteria and/or parameters [redacted] team used during their review; and 4) why [redacted] team reviewed and produced the 296 emails to the House Committee prior to IPS conducting their formal review.

b6  
b7C

[redacted] team used reviewers from the following agencies: 1) Department of Justice (DOJ); 2) CIA; 3) DoD; and 4) White House Counsel (WHC). [redacted] team's POCs were as follows:

b6  
b7C

- DOJ: [redacted] telephone 202 [redacted]
- CIA: When asked directly who the CIA reviewer was, [redacted] and her team stated they did coordinate through the CIA but, to date, had not given a name for who their CIA reviewer was.
- DoD: [redacted] telephone 703 [redacted] email [redacted]@mail.mil.
- WHC: [redacted] telephone 202 [redacted] email [redacted]@who.eop.gov.

[redacted] did not know why [redacted] team used a POC at the DOJ instead of the FBI and a POC at the WHC instead of the NSC. [redacted] did not want to provide his thoughts on why he thought they used the wrong POCs. [redacted] stated that [redacted] team made a "rookie mistake" when they used the WHC instead of the NSC.

b6  
b7C

[redacted] summed up the issue with the different POCs as frustrating and again pointed out that IPS referred the 296 emails to the NSC, FBI, CIA and DoD whereas [redacted] team referred the 296 emails to the WHC, DOJ, CIA and DoD, and none of the referents were known to be the same between IPS' team and [redacted] team.

b6  
b7C

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-13-2016 BY J37J85T94 NSICG

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/24/2015

[redacted]  
[redacted] United States Department of State (STATE), 515 22<sup>nd</sup> Street NW, Washington, D.C. 20037, office telephone (202) [redacted] mobile telephone (202) [redacted] email [redacted]@state.gov, date of birth [redacted] was interviewed in person by FBI Special Agents [redacted] and [redacted] at FBI Headquarters, 935 Pennsylvania Avenue Northwest, Washington, D.C. 20535. After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

[redacted] started working at STATE in [redacted] and since [redacted] was the [redacted] for Margaret "Peggy" GRAFELD, Deputy Assistant Secretary, who was responsible for overseeing 400-500 employees who work on matters related to the Freedom of Information Act (FOIA), the Privacy Act, and information management for STATE. A/GIS was the office that provided guidance, usually through memorandums, that oversaw records compliance for all STATE employees. A/GIS also oversaw the coordination, production and maintenance of STATE's Foreign Affairs Manual (FAM), though A/GIS was not responsible for the FAM's content. [redacted]

b6  
b7C

[redacted] Joyce BARR, Assistant Secretary, Bureau of Administration, was GRAFELD's boss and immediately subordinate to Under Secretary for Management Patrick KENNEDY.

In or around August 2014, [redacted] in Legislative Affairs to work review and production matters related to inquiries from the House Select Committee on Benghazi. [redacted] STATE's Legislative Affairs. It was around that time that [redacted] started to learn about records production and the FOIA process. Around the same time, [redacted] received a telephone call from [redacted] Attorney, Office of the Legal Adviser, who asked [redacted] if there were any CLINTON-related emails in the [redacted].pst file that [redacted] had from a previous FOIA request. [redacted] answered [redacted] that there were CLINTON-related emails in the [redacted].pst file.

b6  
b7C

The Information Programs and Services (IPS), Bureau of Administration oversaw the FOIA program. In or around November or December 2014, in response to a FOIA request, IPS officials were notified they would pick-up 14 banker boxes of emails at former Secretary of State Hillary CLINTON's office related to CLINTON's use of personal email to conduct official STATE business. Later, [redacted]

b6  
b7C

Investigation on 08/19/2015 at Washington, DC

b3  
b7E

File # [redacted] Date dictated N/A

By SA [redacted] SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of Interview [REDACTED], On 08/19/2015, Page 2

[REDACTED] to pick-up only 12 boxes at Williams & Connolly, LLP. On or around December 4, 2014, [REDACTED] picked-up 12 boxes at Williams & Connolly. [REDACTED] and IPS officials were unsure what happened to the other two boxes. The items in the boxes were stacked with no folders or known method of organization.

[REDACTED] Global Publishing Solutions, who used classified copiers and made two-sided copies of all received materials for [REDACTED] a copy for officials in STATE Executive Secretariat (S/ES), and a couple of copies for IPS officials to use for their FOIA review. The original emails were shrink-wrapped and placed in a sensitive compartmented information facility in Newington, Virginia.

In March 2015, [REDACTED] first heard of issues with the CLINTON-related FOIA process. [REDACTED] the FOIA program. The normal FOIA process would be where IPS received a FOIA request, then IPS forwarded that request on STATE forms via email to the person who the FOIA request pertained to. The pertinent party would then fill out the form and provide the IPS office the requested items, which the IPS office then reviewed prior to a release of the information back to the initial requestor. In the CLINTON-related FOIA case, IPS received an unprecedented amount of emails in hard copy form, as there were 52,455 work-related pages to review. In a letter hand-delivered to KENNEDY by Cheryl MILLS, or MILLS' attorney, it was stated, "in an abundance of caution, they overproduced."

Separate from the CLINTON-related FOIA request, there was a Congressional request for CLINTON-related emails related to the Benghazi incident from the House Select Committee on Benghazi. A review was conducted of 296 emails, probably by persons who worked in the Bureau of Legislative Affairs and Office of the Legal Adviser. [REDACTED] stated [REDACTED] and [REDACTED] would know why and how those 296 specific emails were picked and why and how they conducted their own review, separate from any review the IPS unit conducted. Previously, IPS had always been in charge of Congressional document production; [REDACTED] stated attorneys from Legislative Affairs and Office of the Legal Adviser would normally only weigh in on the legality and scope of requests, but IPS would actually conduct the review and production. [REDACTED] and [REDACTED] stated they coordinated the proper review of the material with STATE bureaus and other agencies. After their own review was finished, [REDACTED] and [REDACTED] produced the requested material for the House Committee, prior and independent to the IPS unit's formal review.

[REDACTED] stated those involved at IPS felt the 7<sup>th</sup> floor, or leading STATE officials, had their own ideas on how to formally review the 296 emails. KENNEDY's initial idea for how to review the 296 email was as follows: 1) the IPS officials conduct a review; 2) IPS officials referred items to other STATE bureaus and inter-agency partners for their review; 3) IPS officials received the referral determinations and submitted to the House Committee. The review process that was finally decided upon was as follows: 1) the IPS officials conduct a review; 2) IPS officials referred items to other STATE bureaus and inter-agency partners for their review; 3) IPS officials received the referral determinations and submitted



Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 08/19/2015, Page 3  
 to the Office of the Legal Adviser; 4) after the Office of the Legal Advisers review, then it would be submitted to the House Committee.

b6  
b7c

In mid-March 2015, IPS officials conducted their formal review of the 296 emails on their classified network, aka "CLASSNET," using their Freedoms System, aka "F2." IPS felt immense pressure to complete the review quickly and to not label anything as classified. In IPS' initial review, they did not use a B(1) exemption on any of the emails. The B(1) exemption was used to exclude the public release of classified information or matters related to national security. IPS officials were told there was nothing classified in the 296 emails, so they shouldn't use the B(1) exemption.

However, from the formal review of the 296 emails, in total, \_\_\_\_\_ thought there were four or five STATE bureaus, such as African Affairs Bureau and the Near Eastern Affairs (NEA) Bureau, and five non-STATE agencies, specifically the FBI, CIA, Department of Defense, National Security Council and White House Counsel, that were sent referrals (items/emails) to conduct their own formal classification review. The NEA responded that in the material they received there were four or five B(1) redactions that needed to be made. After he heard this, \_\_\_\_\_ was frustrated and asked IPS officials if they were "going to challenge the desk officer from Maghreb" by using the B(1) exemption. \_\_\_\_\_ asked, "Who at NEA upgraded it? We'll need to explain classification to these people." \_\_\_\_\_ stated multiple times \_\_\_\_\_ already coordinated with other agencies and \_\_\_\_\_ has previous experience with document production." \_\_\_\_\_ stated "NEA will change their B(1)s to B(5)s because they (NEA) didn't understand how to classify items." A B(5) exemption was not used for classified data, but rather for privileged communications, such as executive- or attorney-related privileges. \_\_\_\_\_ or \_\_\_\_\_ also stated, "it's not classified until we upgrade it."

b6  
b7c

The review officials that \_\_\_\_\_ and \_\_\_\_\_ used for the review of the 296 emails were not the same normal review officials that the IPS team use on a regular basis. For example, \_\_\_\_\_ and \_\_\_\_\_ did not use the IPS' normal point of contact for the FBI, \_\_\_\_\_ but instead used someone from the Department of Justice to count as the FBI reviewer. The names \_\_\_\_\_ and \_\_\_\_\_ stated they used for White House Counsel and the Department of Defense were also not the regular reviewers the IPS team used. \_\_\_\_\_ and \_\_\_\_\_ upon being asked directly, would not give a name of who they coordinated reviews with at the CIA.

b6  
b7c

Throughout the process, \_\_\_\_\_ stated if an email/item should have a B(1) exemption, then IPS would use a B(1) exemption. Despite that, at the end of the referral process, IPS was told to run everything by Legislative Affairs and \_\_\_\_\_ IPS officials felt intimidated when they used or suggested the use of the B(1) exemption on any of the 296 emails. In addition to \_\_\_\_\_ and \_\_\_\_\_ KENNEDY and \_\_\_\_\_ were named as some of the STATE officials who pressured IPS employees to not label anything as classified.

b6  
b7c

In late April 2015, IPS officials completed the formal review of the Benghazi-related Congressional inquiry. All materials were ready for release at that time. The CIA provided redactions,

Continuation of FD-302 of [redacted] Interview of [redacted] On 08/19/2015, Page 4

but none were deemed a B(1) exemption. Most of the items with CIA redactions were emails from Sidney BLUMENTHAL. One item was deemed classified according to the FBI and KENNEDY held a closed door meeting attended by the FBI's [redacted] and IPS' [redacted] among others. In that meeting, KENNEDY asked [redacted] to change the FBI's B(1) upgrade classification, but [redacted] did not change the FBI's stance. On May 22, it was decided by the IPS team they would keep the upgrade of the one FBI-related email and the IPS officials sent David KENDALL, Attorney, Williams & Connolly, LLC, a letter informing him of the results.

There was a powerful group of very high-ranking STATE officials that some referred to as "The 7<sup>th</sup> Floor Group" or "The Shadow Government." This group met every Wednesday afternoon to discuss the FOIA process, Congressional records, and everything CLINTON-related to FOIA/Congressional inquiries. The known regular attendees included Jonathan FINER, Chief of Staff for Secretary of State John KERRY, Jennifer STOUT, Deputy Chief of Staff, Heather HIGGINBOTTOM, Deputy Secretary of State for Management and Resources, KENNEDY, Julia FRIFIELD, Assistant Secretary, Legislative Affairs, [redacted] Office of the Legal Adviser, [redacted] Office of the Legal Adviser overseeing STATE's [redacted] [redacted] and [redacted].

Normally, with larger FOIA requests, such as with the CLINTON-related FOIA request, IPS would schedule a rolling release—that meant every few weeks or month, the properly reviewed and approved material would be made public. However, [redacted] [redacted] and The 7<sup>th</sup> Floor Group argued the release should be done all at once in January 2016, for coordination purposes. While IPS officials did not have control of the release process of the 296 emails related to the House Select Committee on Benghazi's request, they did have control for the release process for the approximately 30,000 emails, or 52,455 pages related to the CLINTON FOIA request, and it was decided to be a rolling release.

On July 15, 2015, IPS on-boarded Intelligence Community Inspector General (ICIG) reviewers to help with the overwhelming review process. The ICIG reviewers were trained up and had been integrated into the FOIA review process to help ensure IPS can meet the mandated release of all non-exempt/non-redacted emails by the January 15, 2016 deadline. To date, [redacted] was aware of approximately 305 referrals already sent out for classification determination.

[redacted] stated S/ES are the Custodian of Records for all Secretaries of State and Deputy Secretaries of State. As such, S/ES received all taskers from the IPS team related to FOIA requests that involve Secretaries of State or Deputy Secretaries of State. S/ES should also have answers regarding STATE's procedures that dealt with information technology, including hardware and software for STATE employees' emails and telephones. Joseph MACMANUS, Executive Secretary and Ambassador, S/ES, and [redacted] S/ES, or someone in the S/ES Information Resource Management (S/ES/IRM) unit should know specific details about CLINTON's at-home server set-up. [redacted] stated STATE servers were located at the Enterprise Server Operations Center (ESOC) and Management/IRM (M/IRM) would be knowledgeable about STATE servers.

Continuation of FD-302 of \_\_\_\_\_ Interview of  On 08/19/2015 Page 5

b6  
b7C

High-ranking STATE officials, described as some Assistant Secretaries and all Under Secretaries and higher, used a separate network for emails and record-keeping called the Principal Officer Electronic Management System (POEMS). The vast majority of STATE employees were not on POEMS.

stated he heard third-hand the National Security Agency (NSA) set-up a computer for CLINTON and the FBI should talk to S/ES about the specifics. Additionally, FBI should ask S/ES about Jake SULLIVAN's email being hacked, as maybe that had something to do with CLINTON's emails or why the NSA set-up her computer.

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/31/2015

[redacted] of Platte River Networks, 5700 Washington Street, Denver, Colorado, 80216, telephone (303) [redacted], email [redacted]@platteriver.com, was contacted in person by Federal Bureau of Investigation Special Agents [redacted] and [redacted]. After [redacted] was advised of the identity of the agents [redacted] identified himself as [redacted] Platte River Networks and stated that he had contacted the company's legal counsel about the scheduled meeting with the FBI on July 29, 2015. Counsel had advised [redacted] not to answer questions from the FBI without counsel present.

b6  
b7C

SA [redacted] told [redacted] no interview would be necessary; however, SA [redacted] needed to provide [redacted] a document with instructions for Platte River Networks. [redacted] invited both SAs [redacted] and [redacted] to an empty conference room.

b6  
b7C

SA [redacted] provided a copy of a FBI preservation letter dated July 27, 2015, signed by Charles H. Kable IV, Section Chief, Counterintelligence Division. [redacted] commented company officials had wondered how long it would take for them to be contacted about the named account. [redacted] asked for clarification about the preservation letter and the responsibilities of their company. SA [redacted] then read to [redacted] a portion of the preservation letter and explained the FBI was not asking for any information at this time, but that the letter was served in anticipation of future legal process. The letter requested that Platte River Networks preserve any records to date which were identified in the aforementioned preservation letter. Agents also explained the request for non-disclosure.

b6  
b7C

[redacted] expressed his concern about Platte River Networks becoming a target if this matter ever became public. SA [redacted] provided [redacted] with her contact information at FBI Denver.

b6  
b7C

[redacted] was also provided FBI Strategic Partnership Coordinator (SPC) brochures that have information about Counterintelligence security awareness. Agents also discussed the FBI's Infragard program.

b6  
b7C

Investigation on 07/29/2015 at Denver, Colorado

File # [redacted] Date dictated N/A

b3  
b7E

By SA [redacted] SA [redacted]

b6  
b7C

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/07/2015

On August 6, 2015, KATHERINE M. TURNER, Partner at the law offices of Williams & Connolly LLP, 725 12<sup>th</sup> Street, N.W. Washington, D.C. met at her place of employment with Agents of the FBI pursuant to an agreement reached by correspondence between the Department of Justice and Williams & Connolly. This agreement (enclosed), reached on August 6, 2015, provided that Williams & Connolly voluntarily turn over to the FBI three (3) thumb drives containing 30,490 emails from former Secretary of State Hillary Clinton's @clintonemail.com account as well as hard copy printouts of the emails and a laptop computer containing a duplicate electronic copy.

At approximately 2:30PM, TURNER met Agents at the loading dock of her firm and transferred 22 legal boxes of documents to the FBI's possession along with a laptop computer and three (3) thumb drives described in detail below and on the enclosed FD-941, Consent to Search Computers, and FD-597, Receipt for Property.

Item 1: Lenovo Thinkpad T420, S/N PB-YC912 12/03

Item 2: Lexar Micro 16GB thumb drive, black and silver in color, S/N LTDTT16GB-000-1001DA (original)

Item 3: Lexar Micro 8GB thumb drive, green and white in color, S/N LTDTT8GB-000-117AU

Item 4: Kingston 8GB thumb drive, silver in color, S/N DTSE9

Item 5-27: 22 legal boxes containing paper copies of the above described 30,490 email communications

TURNER explained that the original thumb drive, Item 2, was obtained from Platte River Networks but did not describe how it was collected or under what circumstances. TURNER described the other two thumb drives as identical to the original though one of the drives contained two complete copies of the email set. The laptop computer was previously used by the firm for unrelated matters but was believed

Investigation on 08/06/2015 at Washington, D.C.

File # [REDACTED] Date dictated N/A

By SA [REDACTED]

Continuation of FD-302 of Interview of Katherine M. Turner, On 08/6/2015, Page 2

to have been cleaned of privileged material prior to use and storage of the 30,490 emails. This laptop has not been connected to the internet since being loaded with an electronic copy of the emails. The user name for the laptop is ".\internetonly" and the password is "InternetOnly!!".

TURNER explained that the firm maintains six (6) additional laptop computers, each of which contain identical digital copies of the 30,490 emails, but also contain attorney/client privileged communications and as such are not being turned over to the FBI at this time. TURNER advised her firm is in negotiations with the Department of Justice over the disposition of these laptops.

Prior to departing, TURNER signed the enclosed FD-941, Consent to Search Computers, and FD-597, Receipt for Property. The original was kept by the FBI and copies were made by TURNER for her records.

Subsequent to the FBI's collection of the above, Items 1-27 were transported to the Washington Field Office of the FBI where they were entered into evidence, and given 1B numbers. Copies of the intake sheets and FD-1004 are enclosed with this communication. Items 1-4 were then transported by members of the FBI's Forensic Analysis Unit to Quantico, Virginia for storage and evaluation. Items 5-27 are presently stored in evidence control at the Washington Field Office.

2

Date of transcription 12/21/2015

b6  
b7C

b6  
b7C

b6  
b7C

b1 per DOS

b3  
b7E

BY SA

b6  
b7C

~~SECRET//NOFORN~~

~~SECRET//NOFORN~~

FD-302a (Rev. 10-6-95)

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 12/21/2015, Page 2

b1 per DOS

(S//NF) [REDACTED]

b1 per DOS

(U//FOUO) The communication networks established by the MC team provide the Secretary and his staff with secure data and voice connections, so that they can connect back to the Department of State network to securely conduct official business. Although the networks established by the MC team create encrypted data channels, users are still required to use a fob to access their Department of State email accounts. [REDACTED] noted that the MC team continuously monitors the network encrypters to watch for any signs of an intrusion or other compromise of the system.

b6  
b7C

(U//FOUO) [REDACTED] provided that the Secretary and his team typically do not use the SBU network established by the MC team for personal matters. He noted that they are free to use the standard internet service in their own room, as any other hotel guest would.

b6  
b7C

(S//NF) [REDACTED]

b1 per DOS

When classified documents, or facsimiles, are sent for the Secretary to review they are usually delivered to the MC team by the local U.S. diplomatic establishment. The MC team then reviews the classification markings and page count before providing the document to the recipient. Once the review is complete the MC team collects the document, counts the pages and then enters the event into a log.

(U//FOUO) If an urgent message arrives at the mobile command post for the Secretary or his team the MC team will alert the recipient that a message has arrived and that the recipient should return to the command center. Depending on the Secretary's location, this might mean sending a message to one of his Line Assistants or knocking on his door if it is after hours. [REDACTED] stated that the Secretary does not have a secure cell phone and that he is typically notified to return to the mobile command center even though there are usually secure communications in his car.

b6  
b7C

(U//FOUO) [REDACTED] stated that the MC team's policies and procedures are the same for domestic travel as for international travel. However, in the case of domestic travel the communication kits are sent via Diplomatic Security instead of via the local U.S. diplomatic establishment.

b6  
b7C

~~SECRET//NOFORN~~



~~SECRET//NOFORN~~

FD-302a (Rev. 10-6-95)

Continuation of FD-302 of Interview of [REDACTED], On 12/21/2015, Page 3

b6  
b7C

(U//~~FOUO~~) The MC team is typically staffed by two to four MC team members, depending on the site. All of the MC team members hold a TS/SCI clearance and receive extensive training on the equipment and security procedures before their first deployment. The MC team members are from various components within the Department of State and may be contractors, Foreign Service members, or career civil servants. The average team member is on the team for two or three years before moving on to another assignment within the Department of State. However, [REDACTED] noted that [REDACTED] has been on the MC team for approximately [REDACTED] years.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was not in a position to comment on how the MC policies and procedures had changed between 2009 and today but he noted that they are constantly working to apply faster and lighter technologies that will achieve their mission of providing secure and reliable communications. [REDACTED] had no concerns with the MC team's ability to meet its objectives given the resources that it had. He provided that [REDACTED] or [REDACTED] may be able to provide more insight on how the MC team operated between 2009 and 2011.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

~~SECRET//NOFORN~~

ALL FBI INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 10-12-2016 BY J37J85T94 NSICG ~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1

b3

FD-302a (Rev. 10-6-95)

-1-

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 06/11/2016

(U) ~~(S)~~ On June 10, 2016, [REDACTED] was interviewed by Special Agent (SA) [REDACTED] and SA [REDACTED] at the Central Intelligence Agency (CIA) in McLean, Virginia. Also present for the interview was [REDACTED] CIA attorney in the [REDACTED]. After being advised of the identities of the interviewing agents and the purpose of the interview, [REDACTED] provided the following information:

b3 per CIA

b6

b7C

b3 per CIA

b1 per CIA

b3

b1 per CIA

b3

b1 per CIA

b3

b1 per CIA

b3

Investigation on 06/10/2016 at McLean, VA

File # [REDACTED] ES, SCI Date dictated N/A

by SA [REDACTED] SA [REDACTED]

b3

b7E

b6

b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~ [REDACTED] ~~TOP SECRET~~

b1

b3

FD-302a (Rev. 10-6-95)

~~TOP SECRET~~b1  
b3

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 09/19/2016, Page 2

b3 per CIA

b1 per CIA  
b3b1 per CIA  
b3b1 per CIA  
b3b1 per CIA  
b3

\_\_\_\_\_ did not have any direct knowledge of DoS officials using unclassified or "barely classified" channels \_\_\_\_\_ but he suspected it \_\_\_\_\_

b1 per CIA  
b3

\_\_\_\_\_ Interviewing agents asked \_\_\_\_\_ to review an email \_\_\_\_\_ dated \_\_\_\_\_ and filed \_\_\_\_\_

b1 per CIA  
b3

\_\_\_\_\_ was asked to review another email dated \_\_\_\_\_ and filed \_\_\_\_\_. After reading the email, \_\_\_\_\_ stated that like the previous email, it did not concern him because the email did not reveal details that would compromise source and/or methods.

~~TOP SECRET~~b1  
b3

~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

b3 per CIA

Continuation of FD-302 of \_\_\_\_\_, Interview of \_\_\_\_\_, On 05/10/2016, Page 3

\_\_\_\_\_ reviewed another email dated \_\_\_\_\_ and titled \_\_\_\_\_. After reading the email, \_\_\_\_\_ expressed concerns over the detail contained in the email. \_\_\_\_\_ stated that the email was "very specific," \_\_\_\_\_

b1 per CIA  
b3

\_\_\_\_\_ however, unclassified email should never have been an option.

\_\_\_\_\_ Agents showed \_\_\_\_\_ another email dated \_\_\_\_\_ and titled \_\_\_\_\_. After reviewing the email, \_\_\_\_\_ stated that he did not have concerns over the email as it was related to \_\_\_\_\_

b1 per CIA  
b3

\_\_\_\_\_ Agents showed \_\_\_\_\_ one last email dated \_\_\_\_\_ and titled \_\_\_\_\_. After reviewing the email, \_\_\_\_\_ exclaimed "\_\_\_\_\_ is an idiot." \_\_\_\_\_ further explained he believed the email was "problematic," \_\_\_\_\_

b1 per CIA  
b3

\_\_\_\_\_ expressed his opinion that DoS was not very careful \_\_\_\_\_

b1 per CIA  
b3

(U//FOUO) A copy of the original interview notes and referenced documents is enclosed in a 1A envelope.

~~TOP SECRET~~b1  
b3

6/15/2016 3:34PM

1.3685 P 5

ALL FBI INFORMATION CONTAINED

HEREIN IS UNCLASSIFIED

DATE 10-12-2016 BY J37J85T94 NSICG

~~TOP SECRET~~

~~SECRET~~

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 05/19/2016

(U) ~~(S)~~ On May 17, 2016, [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agent (SA) [redacted] and SA [redacted] at the Central Intelligence Agency (CIA) in McLean, Virginia. Also present for the interview was [redacted] CIA attorney [redacted]. After being advised of the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information:

b3 per CIA

b6  
b7C

b3 per CIA

b1 per CIA  
b3

b1 per CIA  
b3

b1 per CIA  
b3

Investigation on 05/17/2016 at McLean, VA

FBI # [redacted] (TO SCL) Date dictated N/A

by SA [redacted] SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

~~TOP SECRET~~

~~SECRET~~

b1  
b3

~~TOP SECRET~~

FD-302a (Rev. 10-6-95)

b1  
b3

b3 per CIA

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 09/17/2016, Page 2

b1 per CIA  
b3b1 per CIA  
b3b1 per CIA  
b3

\_\_\_\_\_ had no knowledge regarding how State personnel communicated information \_\_\_\_\_ back to State Headquarters (State HQ). However, \_\_\_\_\_ noted the COM had secure communications equipment available. \_\_\_\_\_ had advised State to handle information \_\_\_\_\_ over secure channels, but had concerns the COM would use a non-secure line to call State HQ. \_\_\_\_\_ never directly witnessed this type of communication.

b1 per CIA  
b3

\_\_\_\_\_ After reviewing an email dated \_\_\_\_\_ with the subject line \_\_\_\_\_ Had the email been compromised, the damage would have depended on public speculation regarding the meaning of the email.

b1 per CIA  
b3

\_\_\_\_\_ After reviewing an \_\_\_\_\_ email with the subject line \_\_\_\_\_ stated the inclusion of a location, name, and time in the email was problematic. He would have insisted such an email be handled in classified channels because \_\_\_\_\_

b1 per CIA  
b3~~TOP SECRET~~b1  
b3

FD-302a (Rev. 10-6-95)

~~TOP SECRET~~

[REDACTED]

b1  
b3

Continuation of FD-302 of [REDACTED] Interview of [REDACTED], On 09/17/2015, Page 3

b3 per CIA

[REDACTED] After reviewing an email dated [REDACTED] with the subject line [REDACTED] stated the communication would not be as damaging as the [REDACTED] email.

b1 per CIA  
b3

[REDACTED] After reviewing a [REDACTED] email with the subject line [REDACTED] stated he recalled the situation described in the email [REDACTED]

b1 per CIA  
b3

(U//FOUO) A copy of the original interview notes and referenced documents is enclosed in a 1A envelope.

~~TOP SECRET~~

[REDACTED]

b1  
b3

UNCLASSIFIED//~~FOUO~~

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/21/2016

(U//~~FOUO~~) On June 21, 2016 [redacted] Date of Birth [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at his residence, [redacted] VA. After being advised of the identities of the interviewing agents, and the purpose of the interview [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] worked at the US Department of State (DOS) for approximately [redacted] years before leaving in [redacted] [redacted] telecommunications specialist under the Executive Secretariat (S/ES) at DOS during HILLARY CLINTON's tenure as the Secretary of State. [redacted] noted that his daily duties remained the same during this period despite several reorganizations which moved his position to different departments. He was responsible for supporting the installation and operation of secure communication equipment at DOS. This included secure video, secure voice, the Washfax, as well as regular telephone and facsimile equipment. [redacted] was not responsible for email support, which was the responsibility of S/ES - Information Resource Management (S/ES-IRM). [redacted] reported to [redacted] [redacted] who was the [redacted] S/ES-IRM under JOHN BENTEL.

b6  
b7C

(U//~~FOUO~~) [redacted] supported CLINTON's transition to DOS and was responsible for establishing secure communications in her office, vehicles and residences. He initially conducted a survey at each residence to identify where the commercially provided telecom service entered the residence (i.e., the "point of presence") and to assess what equipment needed to be installed. Thereafter, [redacted] connected a T1 circuit and ran lines to the locations in the residences, where the equipment would be installed. Although [redacted] installed the equipment it was sometimes maintained by other departments within DOS. For example IRM maintained the Defense Red Switch telephones (i.e., red phones) once they had been installed by [redacted]. The point of presence in the Whitehaven residence was in the basement and [redacted] ran lines from there to closet in the third floor SCIF. He then dropped additional lines to the second floor office area so that an additional STE and red phone could be installed. Similarly, the point of presence at the Chappaqua residence was also in the basement and [redacted] ran lines to a small luggage closet and then to the final equipment locations within the residence.

b6  
b7C

(U//~~FOUO~~) During the transition [redacted] was also tasked to research the feasibility of obtaining a secure BlackBerry for CLINTON. [redacted] was directed to do this by a combination of the following people: DAN SMITH (Executive Secretary), LEWIS LUKENS (Deputy Assistant Secretary), JOHN BENTEL (S/ES-IRM Director), and the Operations Center Director who was either [redacted] or [redacted].

b6  
b7C

Investigation on 6/21/2016 at [redacted] VA

File # [redacted] 302 - 82 Date dictated N/A

By SA [redacted]

b6  
b7C  
b3  
b7E  
b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

UNCLASSIFIED//~~FOUO~~



b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 6/21/2016, Page 2

\_\_\_\_\_ at the time. DOS wanted to assess the feasibility of using secure BlackBerry phones because CLINTON and her staff were BlackBerry users so DOS wanted to provide them with resources that they were familiar with. However, after conducting his assessment, \_\_\_\_\_ found that the secure BlackBerry phones would require an entirely new infrastructure, which was cost prohibitive; and the actual devices were too thick.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was shown an email with the subject "State Department Telephone Services at Secretary Clinton's Residence" that he sent to LUKENS and ABEDIN on January 27, 2009. The email summarized the telecom equipment that was installed at the Whitehaven residence. After reviewing the email, \_\_\_\_\_ explained that "CMS VoIP" line referred to the direct phone line to the White House and that the "IST/Red Switch" was a red phone that was installed as a backup to the CMS VoIP line. The "Business Lines" and "Ops Dedicated Drop" were standard phone lines. \_\_\_\_\_ stated that not all of the installed equipment belonged to DOS and noted that the CMS VoIP system belonged to the White House. \_\_\_\_\_ said he did this in an effort to give the Secretary the most reliable equipment but this approach caused some strife within DOS.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ from S/ES-IRM, was responsible for installing and managing CLINTON's computer systems at the residences. \_\_\_\_\_ coordinated his installation activities with S/ES-IRM and typically did not conduct his work when they were on site in effort to avoid flooding the residence with people.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ was shown an email with the subject "Secretary Residential Installation Hotwash" that he sent to BENTEL, \_\_\_\_\_ and \_\_\_\_\_ on March 17, 2009. \_\_\_\_\_ explained that a hotwash was conducted to develop a solution for any technical problems they had or complaints that they received. \_\_\_\_\_ stated that they had significant issues with the unclassified telephone lines at the residence in Chappaqua. He attributed this to the number of service providers that a direct line traversed as it connected Washington and Chappaqua. As a result the lines consistently had bad connections. Additionally, the red phone on the second floor in Chappaqua did not function properly and eventually CLINTON directly asked \_\_\_\_\_ to remove the phone. \_\_\_\_\_ stated that he removed the phone but it created some internal issues for him as the phone was maintained by IRM and not \_\_\_\_\_ group.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ stated that the "Server: Basement Telephone Closet," as listed in the attachment to the aforementioned "Secretary Residential Installation Hotwash" email, referred to the point of presence for the telephone system in Chappaqua and was not a reference to a computer server. \_\_\_\_\_ was aware that there was an email server in the Chappaqua residence. However, he believed it was for the CLINTON's family email and he did not realize that CLINTON was using the server for DOS business.

b6  
b7C

(U//~~FOUO~~) \_\_\_\_\_ could not recall when he first learned that CLINTON was using a private email account but stated that it was sometime during her tenure. He did not think that CLINTON's use of a private email account was odd because COLIN POWELL had a private email account that he accessed from DOS. \_\_\_\_\_ also assumed CLINTON had a DOS issued account. \_\_\_\_\_ did not communicate directly

b6  
b7C

FD-302a (Rev. 10-6-95)

b6  
b7CContinuation of FD-302 of Interview of [REDACTED], On 6/21/2016, Page 3

with CLINTON on email and instead worked through HUMA ABEDIN when necessary [REDACTED] did not recall anybody ever expressing concern over CLINTON's server or email, but noted that he did not attend the S/ES-IRM meetings were such topics would likely have be discussed.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes and referenced documents are attached in a 1A envelope.

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/16/2016

(U//FOUO) On May 12, 2016, [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] in room 374 at the Eisenhower Executive Office Building, 1650 Pennsylvania Avenue NW, Washington, DC 20502. Also present was [redacted] counsel [redacted] attorney at [redacted] and Department of Justice attorney [redacted]. After being advised of the identities of the interviewing agents, and the purpose of the interview [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] is currently employed as the [redacted] at the National Security Council. [redacted] has held a Top Secret/Sensitive Compartmented Information (TS/SCI) clearance since 2003 when he was originally sponsored by the Central Intelligence Agency (CIA). [redacted] is not, nor has he ever been, an Original Classification Authority (OCA). In early [redacted] began a fellowship at the Department of State (DOS) in the South Asia Bureau. After moving to the Iran desk for a few weeks in [redacted] began working as [redacted] for the Special Representative for Afghanistan and Pakistan (SRAP). While at the SRAP office [redacted] worked for PAUL JONES, FRANK RUGGIERO, MARC GROSSMAN and RICHARD HOLBROOKE [redacted] remained working for the SRAP until [redacted] when he moved to [redacted] at DOS.

b6  
b7C

(U//FOUO) While he worked at the DOS, [redacted] was unaware of how information flowed to Secretary of State HILLARY CLINTON. [redacted] was generally aware that the Executive Secretariat at the DOS was responsible for information flow to the Secretary of State. [redacted] could not say who communicated or emailed with CLINTON. [redacted] did not email or communicate with CLINTON directly and did not know that CLINTON had a private email address hosted on a private server until he was made aware via various media outlets in March 2015.

b6  
b7C

(U//FOUO) [redacted] was assigned official DOS email accounts on both an unclassified network and the Secret Internet Protocol Router Network (SIPRNet). [redacted] did not have a Joint Worldwide Intelligence Communications System (JWICS) email account that he could access in his office, but was aware that he was issued one by the Bureau of Intelligence and Research (INR) at the DOS. [redacted] indicated he rarely used his JWICS account because his work did not necessitate it and it was hard to access. [redacted] could not recall any specific DOS training pertaining to official email usage guidelines, policies or practices. [redacted] stated "obviously classified information goes on classified systems."

b6  
b7C

Investigation on 5/12/2016 at Washington, D.C.

b3  
b7E

File # [redacted] 302-85 Date dictated N/A

By SA [redacted]

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 5/12/2016, Page 2b6  
b7c

(U//FOUO) [REDACTED] stated Principal's Committee (PC) meetings were initiated by the National Security Advisor via official notice to government agencies. The PC meetings would involve participating government agencies presenting their policy on topics prescribed by the National Security Advisor. A Deputy's Committee (DC) meeting would involve the same process although convened by the Deputy National Security Advisor. During [REDACTED] tenure at the DOS, he recalled weekly DC meetings related to Afghanistan and Pakistan issues. While in the SRAP office, [REDACTED] would contribute to packages assembled for DC and PC meetings. Usually, the Deputy SRAP would assign various taskings for a policy paper to be used in a DC or PC. Within the SRAP office, [REDACTED] stated there was no science as it related to who was assigned work. The assignments could be based on your area of expertise or who you knew within DOS. [REDACTED] was unaware of any formal process when collaborating, drafting, editing or publishing a written product with another bureau or office at the DOS.

b6  
b7c

(U//FOUO) [REDACTED] was unaware of the term "upclass" as it referred to the classification of a written product. [REDACTED] did not know how classification of a written product was ultimately decided. [REDACTED] recalled seeing written product with suggested classification markings and he would always adhere to those by appropriately marking the same information carried over to his products or edits. [REDACTED] stated portion markings at the DOS were uncommon before WikiLeaks released classified DOS cables on their website. [REDACTED] understood the classification process to "happen organically" and to be "more of an art than a science."

b6  
b7c

(U//FOUO) At this point in the interview, Agents displayed documents and emails concerning a October 5, 2009 PC meeting involving the DOS. [REDACTED] provided the following information:

b6  
b7c

(U//FOUO) [REDACTED] recalled the general topic of the October 5, 2009 PC meeting, but did not recall the exact meeting or any of the displayed documents. [REDACTED] stated there were many PC and DC meetings regarding Pakistan and Afghanistan policy in 2009. [REDACTED] did not recall drafting or editing any portion of the briefing paper or the attachments. [REDACTED] could not recall who drafted any of the briefing paper or the attachments. When shown metadata indicating [REDACTED] drafted the attachments associated with the foregoing briefing paper, [REDACTED] stated the metadata inferred he interacted with the attachments, or possibly saved them at one point, but [REDACTED] did not recall doing so.

b6  
b7c

(U//FOUO) [REDACTED] described the [REDACTED] report as the result of a review of Afghanistan and Pakistan policy requested by General STANLEY MCCHRYSTAL. The report resulted in a request for a troop surge in the area. [REDACTED] recalled there being a classified version of the [REDACTED] report released and then shortly after, an unclassified version released. [REDACTED] believed it was standard practice to have both classified and unclassified versions of a document released around the same time. [REDACTED] described the report as relevant one day, and then shortly after, irrelevant. During his tenure at the SRAP, [REDACTED] could not recall ever reading the [REDACTED] report.

b6  
b7c

(U//FOUO) [REDACTED] recalled having no concerns over classification or mishandling of documents while at the DOS.

b6  
b7c

Continuation of FD-302 of Interview of [REDACTED], On 5/12/2016, Page 3

(U//~~FOUO~~) Notes of the interview and the documents displayed for [REDACTED] will be maintained in an FD340 envelope and filed with the captioned investigation.

b6  
b7C

b6  
b7C

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 2/1/2016

(U//FOUO) On January 29, 2016, [redacted], date of birth [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at Starbucks Cafe, 370 7<sup>th</sup> Ave, New York, NY 10001. Representing [redacted] and also present for the interview, was [redacted], Attorney at Law, telephone (202) [redacted]. After being advised of the identities of the interviewing agents and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] joined the Department of State (DoS) in [redacted] as a Special Assistant for [redacted]. Thereafter she became the [redacted] under JAKE SULLIVAN. [redacted] left the DoS in [redacted] to work for the [redacted].

b6  
b7C

(U//FOUO) [redacted] provided that as a Special Assistant at DoS she was a political appointee. Upon starting at DoS she was sworn in and then received the standard on-boarding and security trainings. However, [redacted] could not recall any specific training about the Freedom of Information Act (FOIA) or the Federal Records Act.

b6  
b7C

(U//FOUO) [redacted] never traveled with CLINTON and had no knowledge of her iPad or other devices that she used. [redacted] did not have direct contact with CLINTON while she was at DoS and did not email directly with her until after she had left DoS. [redacted] knew that CLINTON was using a personal email account but did not know that it was a potential issue until she read about it in the press. [redacted] was unaware of an official policy at DoS regarding the use of personal email accounts and recalled that other people on CLINTON's staff would use their personal emails periodically.

b6  
b7C

(U//FOUO) [redacted] held a TS/SCI clearance while at DoS and received training on the handling of classified information. [redacted] routinely handled classified information on the ClassNet system but did not know how such information was transferred from SULLIVAN or [redacted] to CLINTON.

b6  
b7C

(U//FOUO) ZFS is a Limited Liability Corporation (LLC) that was established for the Office of Hillary Rodham Clinton, by [redacted].

b6  
b7C

(U//FOUO) When [redacted] originally joined the [redacted] it was based in Washington, D.C. at [redacted]. The office then moved to New York City in [redacted].

b6  
b7C

Investigation on 2/1/2016 at New York City, NY

File # [redacted] 302-52 Date dictated N/A

b3  
b7E

By SA [redacted]

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 1/29/2016, Page 2b6  
b7C

[REDACTED] everybody had to work from home until [REDACTED]

b6  
b7C

(U//FOUO) [REDACTED] was originally an [REDACTED] at the [REDACTED] and was primarily responsible for arranging phone calls, drafting memos and summarizing news articles. She was later promoted to the [REDACTED] provided the names and positions of the following individuals who [REDACTED] during that time period:

b6  
b7C

- HUMA ABEDIN – Chief of Staff
- MONICA HANLEY – Personal Assistant

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

b6  
b7C

(U//FOUO) [REDACTED] provided that Platte River Networks (PRN) provided IT support to the [REDACTED] frequently spoke with [REDACTED] from PRN, about routine matters such as purchasing laptops and maintaining the IT systems.

b6  
b7C

(U//FOUO) [REDACTED] had no recollection of ever receiving a laptop from PRN or [REDACTED] spoke with HANLEY regarding this matter approximately one month ago and then reviewed her email records to see if she had any further information about the laptop. [REDACTED] found one email between her and HANLEY in which they discussed sending the laptop to PRN. However, the discussion transitioned from email to phone and [REDACTED] had no further recollection on what occurred. [REDACTED] noted that this occurred during the period when everybody was working from home due to the aforementioned lease issue. Therefore, if the laptop was shipped to her she would have had it sent to her apartment. She further noted that [REDACTED] was responsible for opening the mail for the office but that he would not have opened anything directed to her [REDACTED] speculated that perhaps it was shipped to the Clinton Foundation in New York City but she did not know what they would have done with it.

b6  
b7C

(U//FOUO) [REDACTED] had no recollection of CLINTON's emails being turned over to DoS. Nor was she involved in the culling of CLINTON's emails [REDACTED] had no knowledge of any archives of CLINTON's emails aside from the laptop in question.

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 1/29/2016, Page 3

(U//~~FOUO~~) Following the interview, \_\_\_\_\_ agreed to provide the above referenced email chain with PRN to the FBI. On February 3, 2016, \_\_\_\_\_ counsel electronically provided the email to SA \_\_\_\_\_

(U//~~FOUO~~) A copy of the original interview notes and the email provided by \_\_\_\_\_ are attached in a 1A envelope.

b6  
b7C

b6  
b7C

b6  
b7C



-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 08/10/2015

[redacted] to the Inspector General, United States Department of State, Office of Inspector General (STATE IG), 2121 Virginia Avenue, NW, Suite 8100, SA-3, Washington, DC 20037, telephone (202) [redacted] email [redacted]@state.gov was interviewed in person by FBI Special Agents [redacted] and [redacted]. After being advised of the identity of the interviewing Agents and the nature of the interview [redacted] provided the following information:

b6  
b7C

In early March 2015, the New York Times published an article about Secretary Clinton's personal email account while at the Department of State. The article alleged Secretary Clinton used a personal email account to conduct official government business in violation of federal laws. Sometime thereafter, John KERRY, Secretary of State, sent STATE IG a letter requesting a review of email and records management at the Department of State. On or about March 12, 2015, STATE IG and Office of the Inspector General of the Intelligence Community (ICIG) received letters from Congress requesting a review of State Department employees' use of personal email for official purposes and coordination with relevant agencies to determine whether classified information was transmitted or received by State Department employees over personal systems.

STATE IG initiated a review of the use of personal communications hardware and software by five Secretaries of State and their immediate staffs. The review went as far back as former Secretary Madeleine ALBRIGHT. In Fall 2014, the Department of State wrote to the last four Secretaries of State asking whether they had any official email in their personal records. The Department of State issued preservation requests, asking each former Secretary to preserve all electronic data they had while at the Department of State. Secretary Colin POWELL responded that he used an America on Line (AOL) account. Secretary ALBRIGHT reported that she did not have personal accounts with official records. Secretary Condoleezza RICE reported having a Gmail account, which she did not use for official purposes.

In response to the preservation request, Secretary Clinton's attorney, David KENDALL wrote a letter to STATE IG stating Williams & Connolly, LLP was in possession of three thumb drives with Secretary Clinton's email from her private network. KENDALL and Katherine TURNER were the only people at the firm with access to the thumb drives. The letter further stated Platte River Networks was in possession of the server and had been made aware of the preservation request.

Investigation on 08/07/2015 at Washington, DC

File # [redacted] Date dictated N/A

b3  
b7E

By SA [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; and its contents are not to be distributed outside your agency.



Serial 29

Continuation of FD-302 of Interview of [REDACTED], On 08/10/2015, Page 2b6  
b7c

In December 2014, Williams & Connolly, LLP produced twelve boxes, approximately fifty five thousand pages of about thirty thousand emails to the Department of State from Secretary Clinton's private server. There is a court order in place, which requires all thirty thousand emails to be released by January 30, 2016. The emails have to be released on a monthly basis. The emails are released based on select percentages. Thus far, two waves of Secretary Clinton's emails have been released on the FOIA website. Department of State had about fifty to sixty people working on Secretary Clinton's emails for the FOIA review process.

Upon receipt of the emails, they were scanned, entered to the OCR process and then uploaded to Department's of State ClassNet system, which was classified up to SECRET. The emails were then divided into sub-groups. Then each email went through the FOIA process to determine the appropriate FOIA exemptions, if any. Ultimately, the emails were publicly released. Initially, senior State Department officials were being used to review the emails. The officials would review the email, identify which State Department equity worked on the information, and would then send the email to that department. The receiving department would then identify certain exemptions and/or send to other agencies, if other agency equities were involved. The emails would come back to Department of State for further review and were ultimately reviewed on the FOIA website. The B (1) exemption was used to protect sensitive Department of State equities. B (5) exemptions were used to redact internal deliberations. B (6) exemptions were used to redact Personally Identifiable Information (PII).

STATE IG brought in ICIG to assist with the identification of classified information and to take a look at the FOIA review process. [REDACTED] from ICIG reviewed Department of STATE's FOIA review process. [REDACTED] brought broader experience to Department of State's assembly line review process. [REDACTED] quickly determined Department of State needed to make some changes to their review process. On or about June 19, 2015 STATE IG and ICIG jointly made four recommendations to the State Department related to the FOIA review process. The recommendations were as follows:

b6  
b7c

1. Recommend State Department FOIA office request staff support from IC FOIA offices to assist in the identification of intelligence community equities;
2. Recommend IC FOIA officers review the emails to ensure that ClassNet use is appropriate before transmitting to the State Bureaus for review;
3. Recommend State Department FOIA seek classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified materials; and
4. Recommend State Department FOIA Office incorporate the Department of Justice into the FOIA process to ensure the legal sufficiency review of the FOIA exemptions and redactions.

Patrick KENNEDY, Under Secretary for Management, U.S. Department of State was a key figure in all of this. KENNEDY accepted FOIA recommendations number one and three on behalf of the Department of State. During a July 2015 meeting with STATE IG and KENNEDY, KENNEDY said something to the effect "We sent our folks from Diplomatic Security (DS) to conduct a security

Continuation of FD-302 of Interview of [REDACTED], On 08/10/2015, Page 3b6  
b7C

assessment of Williams & Connolly". DS concluded Williams & Connolly had procedures in place to secure the three thumb drives. KENNEDY mentioned Williams & Connolly handled the General Petreus investigation, so they had the appropriate clearances and were safe. STATE IG left that meeting with the impression that Department of State had an electronic copy of Secretary Clinton's emails. Later, STATE IG was told that Department of State did not have an electronic copy. STATE IG still would like to obtain an electronic copy of the thumb drives.

STATE IG's review focused on the following areas:

- 1) Preservation of Records
  - a. Are records being preserved for archival purposes?
  - b. Are appropriate systems in place for Freedom of Information Act (FOIA) purposes?
  - c. Are records being kept in line with the Federal Records Act?
- 2) On-Boarding Process
  - a. How are methods of communications established for new Secretaries?
  - b. Each Secretary may like various devices, how does Department of State make those devices secure for usage at Department of State?
  - c. How had Department of State addressed security issues?
  - d. How did State Department set up secure phone line at Secretary Clinton's house?
  - e. What precautions were in place for personal devices?
- 3) Records Creation Designation
  - a. How does State Department make sure draft documents get captured in Department of State's records retrieval process?
- 4) How has Department of State handled FOIA and the Congressional Process?

[REDACTED] opined Department of State's record keeping process was not good. Prior to the last couple of years, record keeping was done on a print and file basis. Literally, if someone wanted something to be kept as an official file, that person would have to print the document and request another person file it away. STATE IG was in the process of taking a deep dive into the on-boarding process of Secretary Clinton's server.

b6  
b7C

Secretary Clinton preferred to use Blackberries. In fact, she had at least two email accounts that went directly to her blackberry account. [REDACTED] was not sure whether Secretary Clinton had an Information Technology (IT) infrastructure from her time in the U.S. Senate or her presidential campaign. Bryan PAGLIANO worked in IT support for Secretary Clinton's campaign. Shortly after Secretary Clinton started her tenure at Department of State, PAGLIANO was hired as a Schedule C, directly reporting to Secretary Clinton. PAGLIANO set up Secretary Clinton's personal server and provided her direct IT support. PAGLIANO left the Department of State sometime in 2013 and came back in early 2015 as a contractor. STATE IG contacted PAGLIANO as part of STATE IG's ongoing review. STATE IG was informed PAGLIANO was represented by attorneys from Akin Gump Straus Hauer & Feld, LLP.

b6  
b7C

Continuation of FD-302 of Interview of [REDACTED], On 08/10/2015, Page 4  
PAGLIANO refused to talk without being granted immunity from prosecution.

b6  
b7C

Secretary Clinton had at least two AT&T blackberry accounts. The first account was the HR15 email account. In September 2013, there was an article about Sydney BLUMENTHAL having his email account hacked. Apparently Secretary Clinton's HR15 account was cited in that article. As a result, Secretary Clinton changed her email to HRD14.

[REDACTED] believed that Secretary Clinton's server at some point was held at her Chappaqua residence. Department of State would send an advance team to set up Secretary Clinton's communications wherever she needed. [REDACTED] did not know who paid for the server. Huma ABEDIN and Cheryl MILLS were the conduits for contacting Secretary Clinton. Only a few people at the Department of State were able to contact Secretary Clinton directly.

b6  
b7C

As part of STATE IG's ongoing review [REDACTED]

b6  
b7C

- 1)
- 2)
- 3)

b5 per DOS

[REDACTED] recommended the FBI talk to PAGLIANO, [REDACTED] and [REDACTED] who were all Department of State employees [REDACTED] was willing to provide the FBI with assistance as necessary.

b6  
b7C

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/3/2016

(U//FOUO) On June 3, 2016, Department of State (DoS) [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] in his office located at [redacted] Virginia. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] was the [redacted] from [redacted] to [redacted] to include during the tenure of former Secretary of State CONDOLEEZZA RICE, COLIN POWELL, and HILLARY R. CLINTON at DoS. [redacted] most recently reported to [redacted]

b6  
b7C

(U//FOUO) [redacted] (IT) Operations for DoS. This included, but was not limited to, software applications, hardware, telecommunications, email. [redacted] DoS Information Resource Management (IRM).

b6  
b7C

(U//FOUO) [redacted] provided IT briefings to CLINTON's transition team upon their arrival, however, the DoS executive office did not fall under [redacted] responsibility. JOHN BENTEL, who oversaw Executive Secretariat Information Resource Management (S/ES- IRM), would have been [redacted] in regards to managing IT programs for executive management.

b6  
b7C

(U//FOUO) Around the time of CLINTON's onboard transition, PATRICK KENNEDY, Under Secretary of State for Management, suggested [redacted] interview BRYAN PAGLIANO, who served on CLINTON's 2012 Presidential Campaign. [redacted] and [redacted] interviewed PAGLIANO, who had a MBA from the University of Maryland. After interviewing PAGLIANO, [redacted] agreed he would be a good fit for [redacted] team. PAGLIANO was subsequently hired on to DoS in a Schedule C position, and was tasked with assisting mainly with cost recovery planning and researching DoS technical enhancement opportunities.

b6  
b7C

(U//FOUO) [redacted] was not aware PAGLIANO had a secondary role of providing technical assistance to CLINTON. Although [redacted] was aware PAGLIANO came from CLINTON's campaign, he noted PAGLIANO did not have any overtly apparent ties to the 7<sup>th</sup> floor [a reference to where CLINTON's executive suite was located at DoS]. [redacted] only recalled one incident wherein [redacted] was dealing with a matter that needed input from the 7<sup>th</sup> floor, and PAGLIANO mentioned he occasionally had contact with individuals on the 7<sup>th</sup> floor. PAGLIANO

b6  
b7C

Investigation on 6/3/2016 at [redacted] /A.

b6  
b7C

File # [redacted] 302 Date dictated N/A

b3  
b7E

By SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency and its contents are not to be distributed outside your agency.

b6  
b7C

6/11/16  
Serial 77

b6  
b7CContinuation of FD-302 of Interview of [REDACTED], On 6/3/2016, Page 2

offered to reach out to his 7<sup>th</sup> floor contacts, but [REDACTED] dismissed the offer and proceeded through regular channels. As a Schedule C hire, PAGLIANO would have been required to report any additional income he received from side work with CLINTON.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was not aware of, nor did he have any discussions with PAGLIANO concerning CLINTON's use of a private email account or email server. [REDACTED] did not have direct correspondence with CLINTON, and learned of her use of a private email server when he read about it in the *New York Times*.

b6  
b7C

(U//~~FOUO~~) It was [REDACTED] understanding that DoS policy "discourages" the use of private email, but does not prohibit it.

b6  
b7C

(U//~~FOUO~~) [REDACTED] was not aware of the specific IT setup in either CLINTON's office or her residences. However, he believed both of CLINTON's residences had a DoS Secure Fax. [REDACTED] and/or [REDACTED] may have had knowledge of her office setup. [REDACTED] was assigned to the "help desk," and [REDACTED] worked for [REDACTED] but later went to work on the 7<sup>th</sup> floor. [REDACTED] also assessed [REDACTED] and [REDACTED] may also have more insight as to what DoS IT equipment was installed at both of CLINTON's residences. [REDACTED] was an IRM technician who would know who installed DoS equipment at the Secretary's homes.

b6  
b7C

(U//~~FOUO~~) The State Messaging and Archival Retrieval Toolset (SMART) records management system was implemented by IRM as a result of recommendations from a DoS Executive Steering Committee. SMART replaced DoS's telegraph system, and was developed to automate / streamline the process for archiving records. [REDACTED] was involved in discussions about the development and rollout of SMART, as were representatives from SES. Representatives from the Executive Secretariat asked to be the last to receive the SMART rollout. However, ultimately SMART was never rolled out to the Executive Secretariat. [REDACTED] could not recall exactly when SMART was implemented at DoS, however, he assessed SMART was rolled out sometime in 2007 - 2008.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 5/11/2016

(U//FOUO) On May 10, 2016, [redacted] DOB [redacted] telephone 20 [redacted] SSAN [redacted] was interviewed by Federal Bureau of Investigation (FBI) Special Agents [redacted] and [redacted] at his residence [redacted] MD. After being advised of the identities of the interviewing agents, and the purpose of the interview, [redacted] provided the following information:

b6  
b7C

(U//FOUO) [redacted] served as [redacted] at the Department of State (DoS) from the beginning of KERRY's tenure to [redacted] Prior to joining DoS, [redacted] served as [redacted] when KERRY was the Chairman of the Senate Foreign Relations Committee.

b6  
b7C

(U//FOUO) A lot of information would flow through [redacted] en route to KERRY, to include information concerning Congressional Oversight. [redacted] was tangentially involved in the process of production of DoS records to the Benghazi Committee, in that KERRY asked [redacted] to ensure the Committee did not face any DoS roadblocks in response to the request. Furthermore [redacted] wanted to make certain DoS was as comprehensive as possible in their response to the Committee's request. [redacted] was primarily concerned with KERRY being questioned by the Committee over the totality of the production, and thus wanted to cover every production avenue possible to avoid KERRY being blindsided if called to testify to the Committee. The production of documents related to Benghazi began in the spring (April/May) of 2013 and continued as a "rolling production."

b6  
b7C

(U//FOUO) [redacted] was not aware former Secretary of State HILLARY R. CLINTON was using a private email account until 2013, when he recalled hearing news of her email account potentially being compromised as a result of a hack into Sidney Blumenthal's email account. [redacted] advised KERRY to use a government email account when he became Secretary of State, despite what previous Secretary's may have chosen to do. [redacted] was not aware until recently that CLINTON's private email account was maintained on a private server.

b6  
b7C

(U//FOUO) [redacted] recalled seeing Benghazi production documents containing CLINTON's personal email beginning in early 2014. [redacted] did not recall having any concerns after seeing that CLINTON used a personal email account, as he was aware other Secretary's of State had done the same.

b6  
b7C

Investigation on 5/10/2016 at Washington, D.C.

b3  
b7E

File # [redacted] 302 - 72 Date dictated N/A

By SA [redacted]

b6  
b7C

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 5/10/2016, Page 2

b6  
b7C

(U//~~FOUO~~) In August or September of 2014, \_\_\_\_\_ went to Capitol Hill to meet with the staff members of the Benghazi Committee, in preparation for a pending hearing with KERRY. \_\_\_\_\_ recalled the topic of issue in his meeting with the committee staff surrounded inquiries regarding the preservation of records. Following his meeting with the committee staff, \_\_\_\_\_ contacted CHERYL MILLS to advise of possible leaks from the committee referencing their production concerns related to CLINTON's email. \_\_\_\_\_ recalled at least one phone conversation with MILLS concerning the matter. \_\_\_\_\_ also spoke with \_\_\_\_\_ from a Public Affairs perspective. \_\_\_\_\_ also had some visibility in the matter, as \_\_\_\_\_

b6  
b7C

(U//~~FOUO~~) In approximately December of 2014, \_\_\_\_\_ recalled a large number of printed CLINTON emails being dropped off at DoS. \_\_\_\_\_ was surprised at the volume of emails produced, and believed the production to be close to 50,000 pages. Two attorneys from \_\_\_\_\_ Last Name Unknown (LNU) and \_\_\_\_\_ LNU [believed to be a reference to \_\_\_\_\_ and \_\_\_\_\_], were brought onto DoS to help process and coordinate the redactions in regards to Benghazi FOIA production. \_\_\_\_\_ described \_\_\_\_\_ as someone who would be "encyclopedic" concerning the process of production regarding Benghazi, to include the production of CLINTON's email. DoS \_\_\_\_\_ was also involved with the DoS production and review process as it pertained to CLINTON's emails and Benghazi as a whole. PATRICK KENNEDY, DoS Under Secretary for Management, also had insight into the production process.

b6  
b7C

(U//~~FOUO~~) During the course of the Benghazi production, DoS recognized there was a gap in records related to emails pertaining to not only CLINTON, but other former Secretaries of State who did not use DoS email accounts. As such, Executive Secretary JOSEPH McMANUS drafted a letter in October 2014, requesting former Secretaries produce any personal emails responsive to the Federal Records Act in attempt to retroactively address the gap in DoS records.

(U//~~FOUO~~) \_\_\_\_\_ was not involved with the discussions or the process concerning how the email production was conducted. \_\_\_\_\_ did not provide direction on how the emails should be produced, nor did he have any knowledge of what methodology was used in determining what emails were responsive to production requests. \_\_\_\_\_ was unaware of any concerns that the original production of emails provided by CLINTON was not entirely comprehensive in response to the request, nor was he aware of any concerns that the email production might contain classified material.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes are attached in a 1A envelope.



~~SECRET//ORCON/NOFORN~~

FD-302a (Rev. 10-6-95)

-1-

FEDERAL BUREAU OF INVESTIGATION

Date of transcription 07/23/2015 b3 per ODNI  
b6 per FBI  
b7C per FBI

(U//~~FOUO~~) [redacted] date of birth [redacted] was interviewed at the Office of the Inspector General of the Intelligence Community, Patriot Park, 12290 Sunrise Valley Drive, Reston, Virginia 20191. Also present during the interview were [redacted] and [redacted]. After being advised of the identity of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b3 per ODNI  
b6 per FBI  
b7C per FBI

(U) (~~S//NF~~) [redacted] had worked as an Inspector in the Office of the Inspector General of the Intelligence Community (IC/IG) for approximately 2 years. In May 2015, IG/IC began to assist in the Department of State's Inspector General's (STATE/IG) review entitled "Use of Personal Communications Hardware and Software by Five Secretaries of State and Their Immediate Staffs." This assistance was requested pursuant to the March 12, 2015 letter from the United States Senate.

(U) (~~S//NF~~) On or about May 28, 2015, [redacted] met with [redacted] the Inspector General, United States Department of State (STATE) and other STATE employees in order to assist in completing the review. It appeared that STATE Freedom of Information Act (FOIA) employees were at least already 6 weeks into the review process. [redacted] immediately recognized problems that impeded STATE's review process. Some of the problems were 1) STATE's computer software was at least 2 generations behind; 2) the optical character recognition (OCR) was faulty; and 3) STATE employees used initials to describe organizations, as opposed to using intelligence designations. [redacted] found STATE FOIA employees very helpful. On various occasions many of the FOIA officials stayed after midnight to conduct the email review.

b3 per ODNI  
b6 per FBI  
b7C per FBI

(U) (~~S//NF~~) On or about May 22, 2015, STATE publicly released two hundred ninety-six e-mails belonging to former Secretary of State Hilary Clinton (CLINTON). The two hundred ninety-six e-mails were previously reviewed and released by STATE FOIA officials in response to previous FOIA requests. According to the Defense Intelligence Agency, National Security Agency, and National Geospatial Intelligence Agency officials, at least one of those un-redacted e-mails should have been treated as

Investigation on 07/23/2015 at Reston, Virginia

File # [redacted] Date dictated N/A

By SA [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Classified By: F93M27K51

Derived From: FBI NSIC dated 20130301

Declassify On: 20401231

~~SECRET//ORCON/NOFORN~~

Continuation of FD-302 of Interview of [REDACTED], On 07/23/2015, Page 2 b3 per ODNI  
classified. On or about June 25, 2015 the IC/IG notified the Director of National Intelligence and b6 per FBI  
members of the senate of this leak of classified information. b7C per FBI

(U) ~~(S//NF)~~ IC/IG believed that the release of the two hundred ninety-six e-mails did not comply with FOIA regulations. In fact, public figures were completely redacted from the TO, FROM and CC lines, in violation of FOIA regulations. It also appeared that no STATE FOIA personnel knew how the two hundred ninety-six e-mails had been selected to be released. STATE FOIA personnel indicated during the FOIA review process, some B1 (Classified National Security Information) were removed and changed to B5 FOIA exemptions (Privileged Communications). [REDACTED] believed STATE FOIA redactions of b3 per ODNI  
classified information were inappropriately designated or changed. b6 per FBI  
b7C per FBI

(U) ~~(S//NF)~~ The two hundred ninety-six emails were taken from approximately fifty-five thousand pages of thirty thousand e-mails provided to STATE by the Law Offices of Williams & Connolly LLP, (William & Connolly) CLINTON's personal counsel. According to Williams & Connolly, the firm had provided all of CLINTON's work related or potentially work related e-mails from her @clintonemail.com account. Williams & Connolly also maintained a copy of the .PST file containing the electronic copy of the above referenced e-mails, on a thumb drive, stored in a secure safe at Williams & Connolly's Washington, DC office. David Kendall (KENDALL) and Katherine Turner, Esq. (TURNER) were the only two people that had access to the thumb drive. The firm further advised they believed the server equipment used to host CLINTON's @clintonemail.com account was no longer valid or active. Platte River Networks in Colorado maintained custody of the equipment and had received preservation notices.

(U) ~~(S//NF)~~ IC/IG had considered serving legal process to Williams & Connolly in order to retrieve the thumb drive. Diplomatic Security had attempted to retrieve the thumb drive from William & Connolly, but were informed that since the firm had received preservation letters for the .PST files, the firm could not release the thumb drive to Diplomatic Security. According to [REDACTED] Diplomatic b3 per ODNI  
Security was led to believe Williams & Connolly in fact had 3 copies of the thumb drive. b6 per FBI  
b7C per FBI

(U) ~~(S//NF)~~ In December 2014, Williams & Connolly informed STATE they had fourteen boxes containing the approximately thirty thousand e-mails. However, when STATE officials arrived to pick up the boxes, STATE only received twelve boxes. IC/IG had no information as to whether Williams & Connolly were authorized to store classified information or if KENDALL and TURNER held security clearances.

(U) ~~(S//NF)~~ [REDACTED] surmised [REDACTED] and other STATE FOIA officials b3 per ODNI  
were suspicious of the special appointments to STATE Legislative Affairs of attorneys [REDACTED] b6 per FBI  
[REDACTED] and [REDACTED] and other STATE FOIA personnel believed the b7C per FBI  
involvement of [REDACTED] and [REDACTED] in the FOIA review process was abnormal. [REDACTED] and [REDACTED]  
made recommendations and requested additional changes that were not routine. [REDACTED] and [REDACTED]  
both previously had worked at [REDACTED] which appeared to create a conflict of interest.

b3 per ODNI  
b6 per FBI  
b7C per FBI

Continuation of FD-302 of Interview of [redacted] On 07/23/2015 Page 3

[redacted] believed both attorneys had also worked at the [redacted] and was possibly involved in the Lois Lerner, Internal Revenue Service situation.

b3 per ODNI  
b6 per FBI  
b7C per FBI

(U//~~FOUO~~) On or about June 15, 2015 IC/IG sent a letter to STATE/IG documenting potential issues identified in the Preliminary Review of the State Department FOIA Process. The recommendations were:

1. Recommend State Department FOIA office request staff support from IC FOIA offices to assist in the identification of intelligence community equities;
2. Recommend IC FOIA officers review the email to ensure that ClassNet use is appropriate before transmitting to the State Bureaus for review;
3. Recommend State Department FOIA seek classification expertise from the interagency to act as a final arbiter if there is a question regarding potentially classified materials;
4. Recommend State Department FOIA Office incorporate the Department of Justice into the FOIA process to ensure the legal sufficiency review of the FOIA exemptions and redactions;

b3 per ODNI  
b6 per FBI  
b7C per FBI

(U//~~S//NF~~) On or about June 26-27, 2015, a review of the thirty thousand e-mails revealed five additional classified e-mails. [redacted] used key word searches in order to review the e-mail. It appeared that one in every five e-mail addresses were not a .GOV e-mail address. In the thirty thousand e-mails there were about seventeen unsigned classification upgrade memorandums. These memorandums were packages of information which were being held for the Assistant Secretary of State for Administration's signature.

(U//~~S//NF~~) On or about July 1, 2015, IC/IG officials met with Patrick Kennedy, Under Secretary of State for Management and other STATE representatives. IC/IG informed STATE that IC/IG would assist STATE/IG conduct the review, whether or not STATE welcomed IC/IG's input. [redacted] alleged STATE made several misrepresentations during this meeting. One such statement made by STATE's legal counsel was "there were no classified information contained in the thirty thousand e-mails".

b3 per ODNI  
b6 per FBI  
b7C per FBI

[redacted] was willing to assist the FBI further as needed.

b3 per ODNI  
b6 per FBI  
b7C per FBI

Date of transcription 08/20/2015

[redacted] United States Department of State, Office of Inspector General (STATE IG), 2121 Virginia Avenue, NW, Suite 8100, [redacted] Washington, D.C. 20037, telephone (202) [redacted] email [redacted]@state.gov, date of birth [redacted] was interviewed in person by FBI Special Agents [redacted] and [redacted] in her office. After being advised of the identities of the interviewing Agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

[redacted] began working for STATE IG in [redacted] as [redacted]. In [redacted] she became [redacted] Evaluations and Special Projects unit, which consisted of approximately 10 people from both STATE IG and the Intelligence Community Inspector General (ICIG). [redacted] worked on Congressional requests and other special inquiries that are handled by STATE IG, which included a special project related to the Freedom of Information Act (FOIA) process as a whole.

b6  
b7C

[redacted] STATE IG were in the process of conducting a review at STATE, focused on three main areas. Those areas were how 1) STATE records are preserved; 2) how STATE employees handled the FOIA process; and 3) the on-boarding process for new STATE employees, specific to methods of communication, with an emphasis on the Secretaries of State. As part of that review, [redacted] sent a questionnaire in late March 2015 to the former Secretaries of State Madeleine ALBRIGHT, Colin POWELL, Condoleezza RICE, and Hillary CLINTON along with current Secretary of State John KERRY. The questionnaire specifically asked them about their use of personal email for work purposes.

b6  
b7C

On April 15, 2015 STATE IG sent out requests to a broad number of STATE-related persons, including former staff members and others who may have sent or received work-related emails to or from the personal email accounts of the former Secretaries of State. The request asked for personal emails and any policy or training given related to the use of personal email for business purposes. [redacted] had not yet received any email files from any of the staff members of the former Secretaries of State and was told that there would be no response to the request by the attorney of Bryan PAGLIANO, former information technology advisor for CLINTON.

b6  
b7C

CLINTON sent out an all-staff cable that personal email should not be used day-to-day for business purposes and that personal email is not secure, so do not use them for business purposes. To the

Investigation on 08/19/2015 at Washington, DCb3  
b7EFile # [redacted] Date dictated N/ABy SA [redacted]SA [redacted]b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

Continuation of FD-302 of Interview of [REDACTED], On 08/19/2015, Page 2

best of [REDACTED] recollection, CLINTON sent that cable out in 2009. After CLINTON's time as Secretary of State, there was also STATE guidance that if STATE employees had to use their personal email for business purposes they should send a carbon copy (Cc) to their ".gov" work email as well.

In August 2014, STATE Under Secretary for Management Patrick KENNEDY sent out a memorandum for STATE employees not to use personal email for business purposes, but it did not address whether personal servers may be used for business purposes. There was STATE guidance that all information/emails related to work should be on an "approved automated system," but there was no known STATE guidance regarding the use of personal servers to conduct business. That will be an official "finding" by [REDACTED] colleague [REDACTED] STATE IG.

[REDACTED] stated [REDACTED] interviewed PAGLIANO's former boss while at STATE, and PAGLIANO's former boss was unaware PAGLIANO set-up CLINTON's personal work server for her. There were no on-boarding policies in place to prevent what happened related to CLINTON using a personal server. STATE IG was unsure what, if any, site survey or systems security and maintenance checks were conducted prior to the installation of CLINTON's server by PAGLIANO. STATE IG was also unsure if anyone else other than STATE employees knew of, ever saw, or had access to the server.

All of STATE's top officials' email records related to their ".gov" emails were being preserved, or "journaled," no matter what. Most STATE employees, those not considered top officials, could create email records themselves using the SMART system. The onus was on the regular STATE employees to self-determine what a record is and if they didn't use the SMART system and they've double-deleted the email, it was more than likely not going to be preserved.

Regarding STATE IG's review and interaction with KENNEDY, [REDACTED] had met KENNEDY several times, and stated KENNEDY was never overly uncooperative and never did anything unusual with regards to his cooperation. However, KENNEDY's tone and tenor were definitely not positive when dealing with STATE IG. [REDACTED] also attended meetings with KENNEDY in the past that discussed general goals going forward for STATE with regards to STATE IG's review.

[REDACTED] review led her to interview STATE officials who worked the FOIA process from within the Bureau of Administration, Office of Information Programs and Services, which fell under KENNEDY's purview. Some FOIA officials have seen events and behaviors they did not like or that made them uncomfortable, to include KENNEDY's attitude toward them and how they handled the FOIA process related to CLINTON. Additionally, there was a request from the FOIA officials to STATE employees that asked for any emails sent to or from personal email accounts related to the CLINTON FOIA request. Some STATE employees responded they had no emails that fit the request; despite the negative response, for some STATE employees, FOIA officials knew there were at least some emails that should have been included in their response because the FOIA officials had already reviewed those emails

Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_ On 08/19/2015, Page 3  
from within the batch of 30,000 CLINTON-related emails. Despite knowing some STATE employees had not responded correctly, the FOIA officials had no recourse to compel a positive response.

b6  
b7C

For the FOIA request related to the 30,000 CLINTON-related emails and the Congressional inquiry that requested Benghazi-related emails, those review process were handled outside the normal chain of people. \_\_\_\_\_ did not know why these requests were handled outside the normal chain of people, but \_\_\_\_\_  
b5 per DOS

b6  
b7C

\_\_\_\_\_ recommended the FBI talk to \_\_\_\_\_ for more information on events discussed above and for names of other people the FBI would be interested in talking with regarding the same.

b6  
b7C

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED

DATE 10-12-2016 BY J37J85TS94 NSICG **FEDERAL BUREAU OF INVESTIGATION**

Date of transcription 05/26/2016

(U//~~FOUO~~) On May 25, 2016, [redacted] Special Agent, United States Secret Service (USSS), was interviewed by Federal Bureau of Investigation (FBI) Special Agents (SA) [redacted] and SA [redacted]. Also present for the interview was a Federal Law Enforcement Association (FLEOA) Attorney and USSS SA [redacted]. After being advised of the identity of the interviewing agents and the nature of the interview, [redacted] provided the following information:

b6  
b7C

(U//~~FOUO~~) [redacted] was assigned to the protective detail of WILLIAM CLINTON from [redacted] to [redacted]. Because of [redacted] information technology (IT) skills, he was asked to do network assessments and troubleshoot IT issues at the Clinton Foundation. From [redacted] to [redacted] assisted the Clinton Foundation in a case related to theft of information on the Clinton Foundation information systems.

b6  
b7C

(U//~~FOUO~~) [redacted] was contacted by JUSTIN COOPER in January 2011 to assist with the security of an email server at the Clinton residence in Chappaqua, New York. [redacted] did not physically or remotely access the server in the residence at Chappaqua. [redacted] was not aware of the hardware components of the server or software installed on the server. [redacted] conducted open source research relating to the security of email servers and contacted BRYAN PAGLIANO to recommend adding outbound IP filtering to the server. [redacted] received PAGLIANO's name and contact information from COOPER. [redacted] was aware of no other information pertaining to the email server located in Chappaqua.

b6  
b7C

(U//~~FOUO~~) Notes of the interview will be maintained in a FD340 envelope and filed with the captioned investigation.

Investigation on 05/25/2016 at Boston, Massachusetts

b3  
b7E

File # [redacted] 302 - 93 Date dictated N/A

By SA [redacted]

b6  
b7C

-1-

## FEDERAL BUREAU OF INVESTIGATION

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-12-2016 BY J37J85T94 NSICG

Date of transcription 09/17/2015

On September 17, 2015, [redacted] United States  
Department of State (DoS), 2025 E. Street NW, Washington, D.C. 20520, was interviewed by FBI  
Special Agent [redacted] and Information Technology Specialist / Forensic Examiner [redacted]  
[redacted] Also present was [redacted] DoS, office telephone  
202 [redacted] After being advised of the identity of the interviewers and the nature of the interview  
[redacted] provided the following information:

b6  
b7c

The DoS email system uses a hub and spoke configuration. There are approximately 120,000 mailboxes on the system, of which approximately 95,000 are for unique users. The other 25,000 mailboxes are general mailboxes and aren't assigned to a specific user. Approximately 35,000 mailboxes reside on the local hub and are administered by Information Resource Management (IRM). The remainder of the mailboxes reside on spokes within the system and are not controlled by IRM. Spoke mailboxes, such as those at overseas posts, are administered by the local Information Security Officer and backup procedures vary by site.

Upon receiving the preservation request from the FBI, IRM preserved and thereafter exported the mailboxes for all of the individuals listed on the request whose mailboxes are on the IRM system. [redacted] estimated that approximately 400 of the 900 accounts listed on the preservation request are active users on the IRM system, with the other accounts residing on spokes, POEMS, or are associated with users who are no longer at DoS. Each exported mailbox includes all of the active mail folders as well as any items in the Recoverable Items storage area of Microsoft Exchange, which retains items for 90 days after they are deleted by the user. The export does not include any files, or mailboxes, that may have been archived by the user to their local desktop.

b6  
b7c

The IRM operating system is backed up and retained for approximately 30 days. However, the email database is not part of the backup. For email recovery, IRM uses Database Availability Groups (DAG) whereby five dynamic copies of each mailbox are maintained, at two sites, to allow the system to be quickly restored if the primary database fails.

[redacted] opined that the exported mailboxes were unlikely to contain many emails from prior to 2012. Prior to that time mailboxes were limited to 500MB of data and users were regularly required to

b6  
b7c

---

Investigation on 09/17/2015 at Washington, DCb3  
b7EFile # [redacted] 302 - 6 Date dictated N/ASA [redacted]  
By ITS/FE [redacted]b6  
b7c

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.



Continuation of FD-302 of \_\_\_\_\_ Interview of \_\_\_\_\_, On 09/17/2015, Page 2

b6  
b7C

delete old emails, or to create Personal Storage Folders (.pst files), when they hit the storage limit. Between 2012 and 2013, the storage limits were increased to 5GB.

IRM uses the State Messaging and Archival Retrieval Tool (SMART) to archive record emails. The system was implemented in phases between 2008 and 2010 and replaced CableXpress for archiving cables and record emails. \_\_\_\_\_ noted that communications sent to an embassy are referred to as a cable and emails sent to a person are record emails. SMART requires the users to identify an email as meeting the record standard and then selecting the appropriate SMART tags within Outlook while composing the email. The period of retention for a SMART record is dependent on the tags selected by the user.

b6  
b7C

\_\_\_\_\_ provided that S/ES-IRM, also commonly referred to as the POEMS system, does not use the SMART system to archive email records. They are instead obligated to follow the 'print and file' policy. \_\_\_\_\_ further noted that records for senior officials are archived when they leave office. \_\_\_\_\_ recommended contacting Deputy Assistant Secretary MARGERET (PEGGY) GRAFELD, Deputy Assistant Secretary for Global Information Services (A/GIS) for more information on this process.

b6  
b7C

The Bureau of Intelligence and Research (INR) is responsible for administering the mailboxes on the top secret network at DoS. \_\_\_\_\_ provided that \_\_\_\_\_ telephone 202 \_\_\_\_\_ would be able to provide further details on INR and the top secret mail system.

b6  
b7C

♦♦

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED

DATE 10-12-2013 BY J37J85T94 NSICG **FEDERAL BUREAU OF INVESTIGATION**

Date of transcription 09/22/2015

On September 21, 2015, [redacted] United States Department of State (STATE), Office of Inspector General (OIG), Office of Investigations, 1700 N. Moore Street, Suite 800, Arlington, VA 22209, office telephone 703 [redacted] fax 703 [redacted] email address [redacted]@state.gov called the writer, Information Technology Specialist/Forensic Examiner (ITS/FE) [redacted] of the Washington Field Office (WFO) Computer Analysis Response Team (CART).

b6  
b7C

The writer asked [redacted] to provide general information regarding a group of fifty (50) email messages of interest that were found by [redacted] during his review of the Microsoft Outlook Personal Storage Folders (.pst files, or "mailboxes") for HUMA M. ABEDIN and CHERYL D. MILLS. [redacted] confirmed that the Federal Bureau of Investigation (FBI) previously received a full copy of the two (2) mailboxes on a Lexar thumb drive provided by [redacted] from STATE.

b6  
b7C

[redacted] stated that he performed a search across the email data for the words "Secret" and "NOFORN" using a search program called "Perceptive Search" and that the search returned fifty documents of interest. [redacted] believed that most of the search hits appeared within the metadata of Microsoft Word documents, which he identified as "Call Sheets," or documents provided to the Secretary of State prior to attending briefings with foreign dignitaries. [redacted] believed the search hits appeared within the metadata of the documents and not within the actual content of the documents. The identified documents were sent as attachments to emails. [redacted] could not remember if there were also search hits within any email messages.

b6  
b7C

[redacted] believed that the documents may have been generated from a classified system and that at some point they may have been moved to an unclassified system. However, he was unsure whether the "Secret" and "NOFORN" markings would have been generated automatically by the system that was used to create the documents. [redacted] stated that STATE had not yet determined how the documents would have been marked with regard to classification.

b6  
b7C

The writer requested that [redacted] provide the FBI with the file names and Message-Digest algorithm 5 (MD5) hash values for the files identified by STATE. [redacted] advised that STATE was in the process of moving the email data onto a stand-alone computer within a Sensitive Compartmented Information Facility (SCIF) and that he anticipated this would happen

b6  
b7C

Investigation on 09/21/2015 at Washington, DC

b3  
b7E

File # [redacted] 302 - 3 Date dictated N/A

By ITS/FE [redacted]

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.

b6  
b7C

b6  
b7C

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED  
DATE 10-12-2016 BY J37J85T94 NSICG

## FEDERAL BUREAU OF INVESTIGATION

Date of transcription 6/23/2016

(U//~~FOUO~~) On June 23 2016 [REDACTED], date of birth [REDACTED] was telephonically interviewed by Federal Bureau of Investigation (FBI) Special Agents [REDACTED] and [REDACTED]. Also present for the call was [REDACTED] counsel [REDACTED] Attorney at Law. After being advised of the identities of the interviewing agents and the purpose of the interview, [REDACTED] provided the following information:

b6  
b7C

(U//~~FOUO~~) [REDACTED] had no new information regarding the whereabouts of the laptop that was shipped by [REDACTED] from Platte River Networks (PRN) to the Clinton Foundation in April of 2014. [REDACTED] was not sure who the mailroom manager for the Clinton Foundation was at that time but offered to contact the foundation to inquire about the shipment. [REDACTED] confirmed that the address of the Clinton Foundation was 1271 Avenue of the Americas, 42<sup>nd</sup> Floor, New York, NY 10020.

b6  
b7C

(U//~~FOUO~~) Following her January 2016 interview, [REDACTED] provided the FBI an email chain from April 2014 with the subject "RE: HRC emails." [REDACTED] had not reviewed the email chain prior to this call and could not immediately access the email so the interviewing agent read the chain to [REDACTED] to refresh her memory. Upon hearing the content of the email, [REDACTED] provided that she recalled having a discussion with [REDACTED] about remotely accessing the HILLARY CLINTON email archive via the internet. However, [REDACTED] could not recall if she actually accessed the email archive remotely thereafter. [REDACTED] believed that she may have taken notes about the process during the call and agreed to check her personal records for any relevant information.

b6  
b7C

(U//~~FOUO~~) A copy of the original interview notes and the referenced email are attached in a 1A envelope.

Investigation on 6/23/2016 at Washington, DCFile # [REDACTED] 302 -84 Date dictated N/ABy SA [REDACTED]b3  
b7Eb6  
b7C

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIEDDATE 10-12-2016 BY J37J85T94 NSICG **FEDERAL BUREAU OF INVESTIGATION**Date of transcription 10/27/2015

On October 27, 2015, [ ] a Special Agent with Homeland Security Investigations (HSI), Department of Homeland Security (DHS), Norfolk Virginia, (757) [ ] was interviewed at the Norfolk Federal Building. After being advised of the identity of the interviewing Agent and the nature of the interview, [ ] provided the following information:

b6  
b7c

[ ] was previously employed as an Agent at the Department of State, Bureau of Diplomatic Security (DS), and assigned to former Secretary of State Rice's personal protection detail from [ ] until January 2009. In January 2009 he was reassigned to former Secretary of State Clinton's detail. [ ] served on Clinton's detail until [ ] when he left the Department of State.

b6  
b7c

Clinton's tenure at State brought about significant changes to established security and diplomatic protocols owing to the dissimilar management styles and attitudes between Rice and Clinton. [ ] claimed that his time on Clinton's detail was short and that he had no information to offer with regard to security violations or mishandling of classified information on the part of Clinton or her staff. [ ] advised his recollections were vague regarding his time on Clinton's detail and that he could not recall specific events with clarity. [ ] was aware that a Blackberry phone was kept in a desk drawer in Clinton's SCIF but could not say with any degree of certainty that the phone belonged to Clinton or that storing it in the SCIF was a security violation. [ ] provided the name of [ ] a former ASAC on Clinton's security detail as someone who may be in a position to provide additional insight. [ ] was not familiar with the current whereabouts of [ ]

b6  
b7cInvestigation on 10/27/2015 at Norfolk, VAb3  
b7EFile # [ ] - 302 - 26 Date dictated N/ABy SA [ ]b6  
b7c

ALL FBI INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED

DATE 10-12-2016 BY J37J85T94 NSICG **FEDERAL BUREAU OF INVESTIGATION**

Date of transcription 11/06/2015

On November 6, 2015, [redacted] Senior Special Agent,  
Office of Investigations, Office of the Inspector General (OIG), United States Department of State  
(STATE), office telephone 703 [redacted] cell 202 [redacted] email address  
[redacted]@state.gov called the writer, Information Technology Specialist/Forensic Examiner  
(ITS/FE) [redacted] of the Washington Field Office (WFO) Federal Bureau of Investigation  
(FBI) Computer Analysis Response Team (CART).

b6  
b7C

[redacted] stated that he located an email containing content from a "confidential cable"  
sent from a Microsoft "Hotmail" email account to the STATE email address for Huma Abedin  
(AbedinH@state.gov) that could be found in the data contained within evidence item 1B26  
provided by STATE to the FBI on or around August 14, 2015. Evidence item 1B26 is further  
described as a white and grey Lexar USB 3.0 thumb drive labeled with a sticker containing the  
words "Dept of State 703-312-3856." [redacted] stated that when the email was received in 2011,  
the information was classified and that it was supposed to be declassified in 2013 but that he did  
not know if that was the case and did not know the current classification of the document.

b6  
b7C

On November 6, 2015, [redacted] sent the writer an email containing information to assist  
in locating the identified email in the FBI data set in evidence item 1B26. A copy of the email is  
included in a 1A envelope.

b6  
b7C

Investigation on 11/06/2015 at Washington, DC

b3  
b7E

File # [redacted] 02-27 Date dictated N/A

By ITS/FE [redacted]

b6  
b7C

This document contains neither recommendations nor conclusions of the FBI. It is the property of the FBI and is loaned to your agency; it and its contents are not to be distributed outside your agency.