remotely.[364,365,366] 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.[yy,367,368]

(U//~~FOUO~~) Investigation indicated that on March 25, 2015, PRN held a conference call with President Clinton's staff.[369,370] In his interviews with the FBI, ndicated 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.[371] In his FBI interview on February 18, 2016 indicated that he did not recall conducting deletions based upon this realization.[372] 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.[373] Investigation found evidence of these deletions[374] and determined the Datto backups of the PRN Server were also manually deleted during this timeframe.[375] Investigation identified a PRN work ticket, which referenced a conference call among PRN, Kendall, and Mills on March 31, 2015.[376,377] PRN's attorney advised not to comment on the conversation with Kendall based upon the assertion of the attorney-client privilege.[378]

(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.[379,380] advised during his February 18, 2016 interview that he did not recall seeing the preservation request referenced in the March 9, 2015 e-mail.[381] 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.[382] 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.[383] Mills stated she was unaware that had conducted these deletions and modifications in March 2015.[384] Clinton stated she was also unaware of the March 2015 e-mail deletions by PRN.[385]

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[zz] from Clinton's tenure containing Clinton's hdr22@clintonemail.com[aaa] e-mail address that were not provided by

[yy] (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.

[zz] (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.

[aaa] (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.

SECRET//~~ORCON~~/NOFORN

b1
b3
b7E

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

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.[386,387,388] 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.[ccc,389] State determined that the other two e-mail chains are currently UNCLASSIFIED.[390,391] 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.[ddd,392] 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.[393] Clinton did not believe the content of the e-mail was classified and questioned the classification determination.[394] 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.[395]

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[ccc] 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

---

[bbb] (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.

[ccc] (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.

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

[eee] (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.

SECRET//~~ORCON~~/NOFORN

b1
b3
b7E

HRC-20

~~SECRET//ORCON/NOFORN~~ [redacted] b1 b3 b7E

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).[fff] 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). [redacted] 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~~ [redacted]

- (S//~~OC/NF~~) [redacted]
- (S//~~OC/NF~~) [redacted]
- (S//~~OC/NF~~) [redacted]
- (S//~~OC/NF~~) [redacted] b1 b3
- (S//~~OC/NF~~) [redacted]
- (S//~~OC/NF~~) [redacted]
- (S//~~OC/NF~~) [redacted]
- (S//~~OC/NF~~) [redacted]

(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

[fff] (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.

~~SECRET//ORCON/NOFORN~~ [redacted] b1 b3 b7E

b1
b3
b7E

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.[ggg,hhh] 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].[iii] 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.[jjj] 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].[kk]

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.[396,397,398,399,400,401,402,403,404,405,406,407,408] 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.

[ggg] (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.

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

[iii] (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.

[jjj] (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.

b6
b7C

[kkk] (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").

b1
b3
b7E

b1
b3
b7E

Individuals who worked in the State Bureau of Public Affairs[lll] often accessed classified information to understand the context of unclassified information that was to be disseminated publicly.[409] 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.[410] The Public Affairs officials were also responsible for notifying State leadership of impending reports by the news media regarding sensitive or controversial topics.[411] 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.[412]

(U//~~FOUO~~) Individuals, including those in the State Operations Center (Ops Center),[mmm] 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.[413,414] 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.[nnn,415,416]

(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.[417,418,419,420] 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.[421,422,423,424] [redacted] stated that [redacted]

b1
b3
b6
b7C

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

[lll] (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."

[mmm] (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.

[nnn] (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.

b1
b3
b7E

that way." [429] 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" classified information.[430,431,432,433] stated the information in the former declined to comment on the e-mails.[435] 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."[436] Sullivan indicated he had no reason to believe any State employee ever intentionally mishandled classified information.[437]

(S//~~OC/NF~~) The FBI interviewed four USIC executives stationed both in the United States and overseas.[438,439,440,441] The USIC executives reviewed the e-mail chains which transited Clinton's personal e-mail account and assessed that some of the e-mail chains should be considered classified.[442,443,444] [445] However, two of the USIC executives interviewed said some of the

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

(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.[455] Mills also stated that she was not concerned about her decision to forward certain of these e-mails to Clinton.[456] 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.[457]

(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.[458] 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.[459] Sullivan also indicated that, for some of the e-mails, information about the incidents described therein may have already appeared in news reports.[460] Furthermore, Sullivan stated that his colleagues at State worked hard while under pressure and used their best judgment to accomplish their mission.[461] 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.[462] 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.[ooo,463]

(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.[464] 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."[465] 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.[466] [redacted] b1 b3

[redacted]

(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.[470] 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.[ppp,471]

(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-

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

[ppp] (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[qqq] 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.[472,473] 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.[474,475,476,477,478,479,480,481,482,483,484,485,486,487] The memos contained a notation of "CONFIDENTIAL"[rrr] and then often included a source summary statement[sss] similar to those frequently found in USIC intelligence products.[488,489,490] 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.[491] 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.[492,493] According to e-mails between Clinton and Sullivan, Clinton discussed passing the information to the White House, other USG agencies, and foreign governments.[ttt,494,495]

E. (U ~~//OUO~~) 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.[496] 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.[497] Clinton believed information should be classified when it relates to [redacted] the use of sensitive sources, or sensitive deliberations.[498] 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."[499] b1 b3

(U) (~~S~~//~~OC/NF~~) Clinton did not recall receiving any e-mails she thought should not have been on an unclassified system.[500] 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.[501] 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.[502] Upon reviewing an e-mail classified SECRET//NOFORN dated December 27, 2011, Clinton stated no policy or practice existed

[qqq] (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.
[rrr] (U//~~FOUO~~) According to Blumenthal, "CONFIDENTIAL" meant the memo was personal in nature and did not refer to classified USG information.
[sss] (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.
[ttt] (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.

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.[503] 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.[504] When asked, Clinton recalled being briefed on SAP information but could not recall any specific briefing on how to handle SAP information.[505] Clinton stated she knew SAP information was of great importance and needed to be handled carefully.[506]

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[uuu] and Hurricane Sandy[vvv]. 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[www] 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.[507,508] The certificate was valid until September 13, 2013, at which time PRN obtained a new certificate valid until September 13, 2018.[509]

(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

b1 b3 b7E b6 b7C

[uuu] (U//~~FOUO~~) The first of two extended outages occurred from August 28 to 30, 2011 (3 days) as a result of Hurricane Irene.
[vvv] (U//~~FOUO~~) The second extended outage occurred from October 30, 2012 to November 9, 2012 (11 days) as a result of Hurricane Sandy.
[www] (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.

b1 b3 b7E

surprised if classified information was being transmitted to Clinton's personal server.[510] further recommended that e-mail transiting from a state.gov account to the server should be sent through a Transport Layer Security (TLS)[xxx] tunnel.[yyy] Pagliano advised that the transition to TLS never occurred.[511,512] The FBI was unable to forensically determine if TLS was implemented on the Pagliano Server.

(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.[zzz,513] 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.[514] Pagliano knew the attempts were potential attackers because the credentials attempting to log in did not match legitimate users on the system.[515] Pagliano could not recall if a high volume of failed login attempts emanated from any specific country.[516]

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

[xxx] (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.

[yyy] (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.

[zzz] (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.

[aaaa] (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.

[bbbb] (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.

[cccc] (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.

[dddd] (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.

b1
b3
b7E

on a server is convenient for remote access, the FBI is aware of known vulnerabilities[cccc] associated with the protocol.

b3

(U//FOUO) [redacted] [523,524] Pagliano recalled finding "a virus," but could provide no additional details, other than it was nothing of great concern.[525] FBI examination of the Pagliano Server and available server backups did not reveal any indications of malware.[526]

(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.[527] Cooper sent Abedin another e-mail later the same day stating he had to reboot the server again.[528] The FBI's investigation did not identify successful malicious login activity associated with this incident.[529]

(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.[530] Forensic analysis noted that on January 5, 2013, three IP addresses matching known Tor[ffff] exit nodes were observed accessing a user e-mail account on the Pagliano Server believed to belong to President Clinton staffer [redacted] FBI investigation indicated the Tor user logged in to [redacted] e-mail account and browsed e-mail folders and attachments.[531,532] When asked during her interview, [redacted] stated to the FBI she is not familiar with nor has she ever used Tor software.[533] FBI investigation to date was unable to identify the actor(s) responsible for this login or how [redacted] ogin credentials were compromised.[534]

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.[535]

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

[cccc] (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.
[ffff] (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.
[gggg] (U) A domain controller is a Microsoft server that responds to security authentication requests (logins, checking permissions, etc.) within a Windows domain.

b1
b3
b7E

b1
b3
b7E

increase in unauthorized login attempts into the Apple iCloud[hhhh] account likely associated with Clinton's e-mail address[iiii] during this time period. Investigation determined all potentially suspicious Apple iCloud login attempts were unsuccessful.[538] 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.[539] Staff also discussed the possibility of conducting penetration testing[iiii] against the PRN Server to highlight vulnerabilities in the network.[540] 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.[541]

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.[542,543,544,545] The FBI forensically examined two of the three iPads[kkkk] it obtained and found no evidence of cyber intrusion.[546]

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.[547] [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.[552] Clinton replied to the e-mail [redacted] stating, "Is this really from you? I was worried about opening it!"[553] [redacted] In a separate incident [redacted] Abedin sent an e-mail to [redacted] indicating Clinton was

b1
b3
b6
b7C

[hhhh] (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.

[iiii] (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.

[jjjj] (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.

[kkkk] (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.

[llll] (U) RAT is a piece of software that facilitates remote operation of a computer system.

b1
b3
b7E

b1
b3
b7E

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.[554] 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.[560.56] [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.[563] 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."[564] Clinton's immediate staff was also briefed on cybersecurity threats in April and May 2011.[565]

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

b1
b3
b6
b7C
b7E

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

b1
b3
b6
b7C
b7E

[554] (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.
[555] (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.

HRC-31

b1
b3
b7E

SECRET//~~ORCON~~/NOFORN [redacted] b1 b3 b7E

(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.[587] [redacted] b7E [redacted][588] One of the screenshots captured a list of 19 foreign policy and intelligence memos authored by Blumenthal for Clinton.[589] The content of one of the memos on the list was determined by State to be classified at the CONFIDENTIAL level.[590] Lazar was extradited from Romania to the United States on March 31, 2016.[591]

(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.[592] On May 26, 2016, the FBI interviewed Lazar, who admitted he lied to FOX News about hacking the Clinton server.[593] 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.[594] 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.[595] However, none of these attempts were successful, and it could not be determined whether this activity was attributable to Lazar.[596]

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. [redacted] b1 b3 b6 b7C b7E

(U//~~FOUO~~) FBI extracted the Thread-Index[oooo] and Message-ID[pppp] values for each identified confirmed classified e-mail relevant to this investigation. The values were extracted from the e-mail headers[qqqq] 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][rrr]. The FBI also provided the unique identifiers to other government agencies, and one entity b7E

[oooo] (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.
[pppp] (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).
[qqqq] (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.
[rrr] (U//FOUO) [redacted] b7E

SECRET//~~ORCON~~/NOFORN [redacted] b1 b3 b7E

~~SECRET//ORCON/NOFORN~~ [redacted]

b1
b3
b7E

responded.[ssss] To date, the signature-based searches in USG databases have not identified the relevant e-mails.[601]

[ssss] (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.

~~SECRET//ORCON/NOFORN~~ [redacted]

b1
b3
b7E

b1
b3
b7E

SECRET//~~ORCON/NOFORN~~

b3
b5
b6
b7C
b7E

(U)

SECRET//~~ORCON/NOFORN~~

HRC-34

b1
b3
b7E

b1
b3
b7E

SECRET//~~ORCON/NOFORN~~

(U)

b3
b5
b6
b7C
b7E

SECRET//~~ORCON/NOFORN~~

HRC-35

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

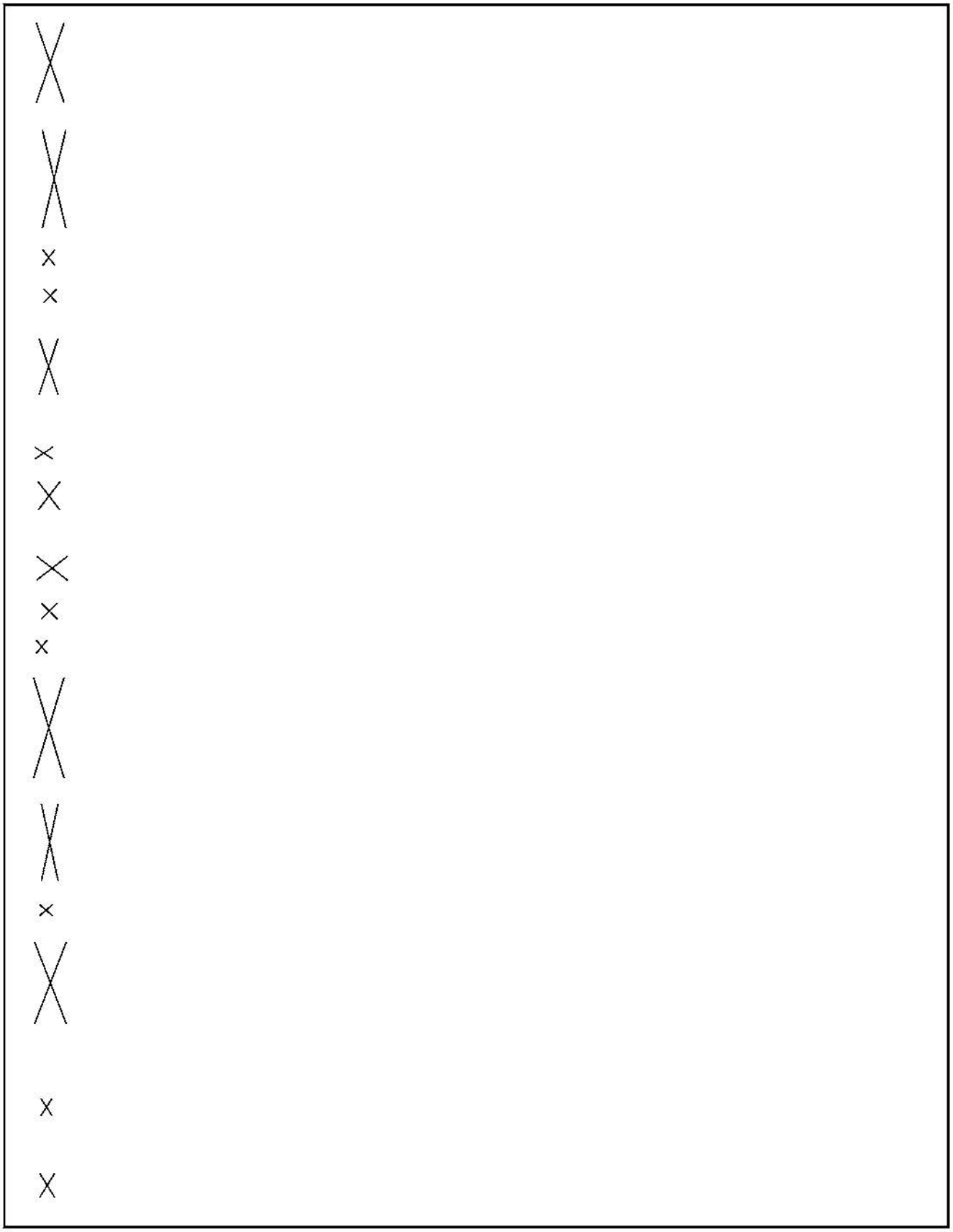
b1
b3
b5
b6
b7C
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E



b1
b3
b5
b6
b7C
b7E

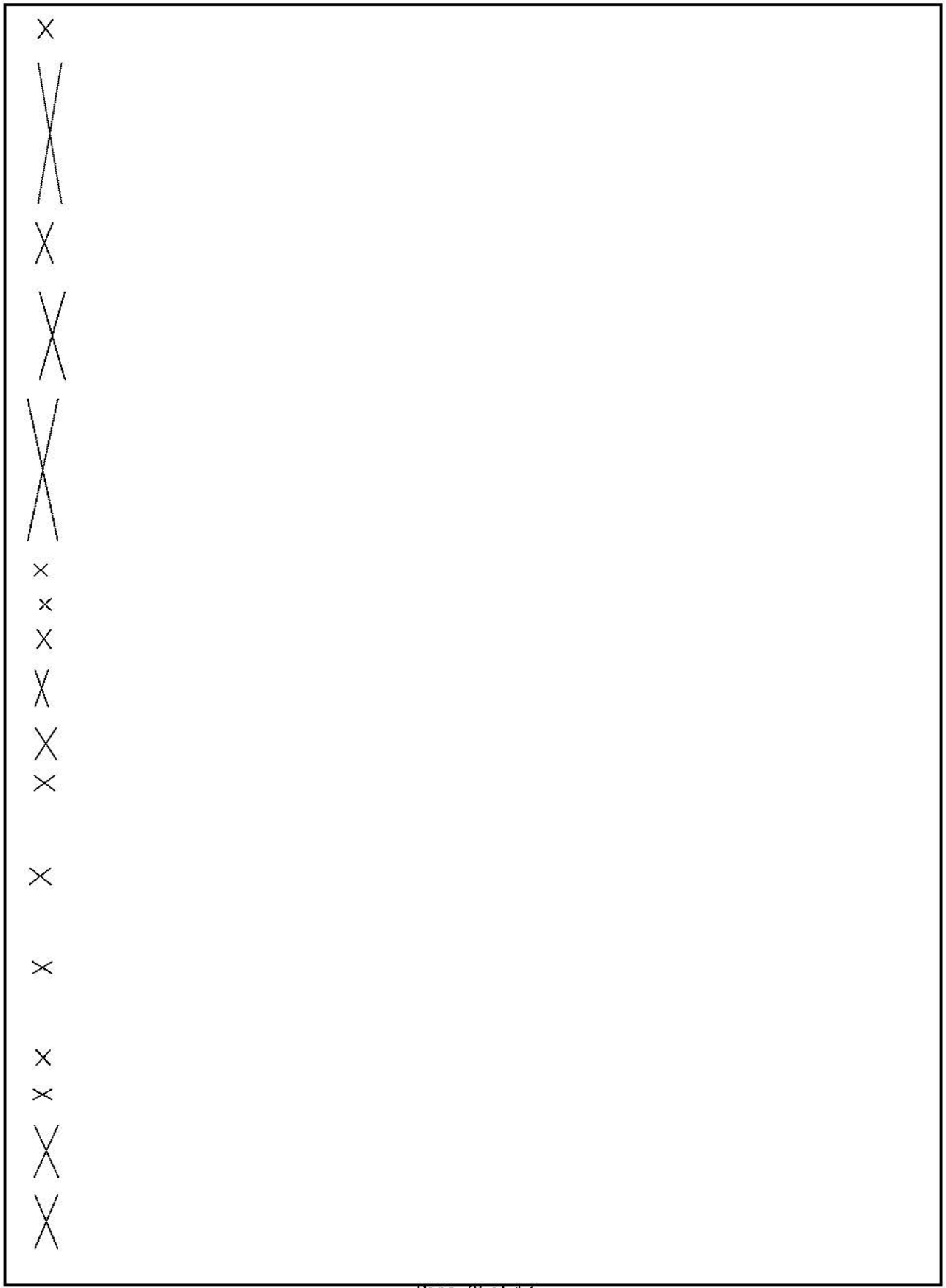
SECRET//ORCON/NOFORN

HRC-37

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E



b3
b5
b6
b7C
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

b1
b3
b7E

SECRET//ORCON/NOFORN

b3
b5
b6
b7C
b7E

SECRET//ORCON/NOFORN

HRC-39

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

(U)

b3
b5
b6
b7C
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

SECRET//~~ORCON/NOFORN~~

b1
b3
b7E

(U)

b3
b5
b6
b7C
b7E

SECRET//~~ORCON/NOFORN~~

b1
b3
b7E

~~SECRET//ORCON/NOFORN~~

b1
b3
b7E

(U)

b3
b5
b6
b7C
b7E

~~SECRET//ORCON/NOFORN~~

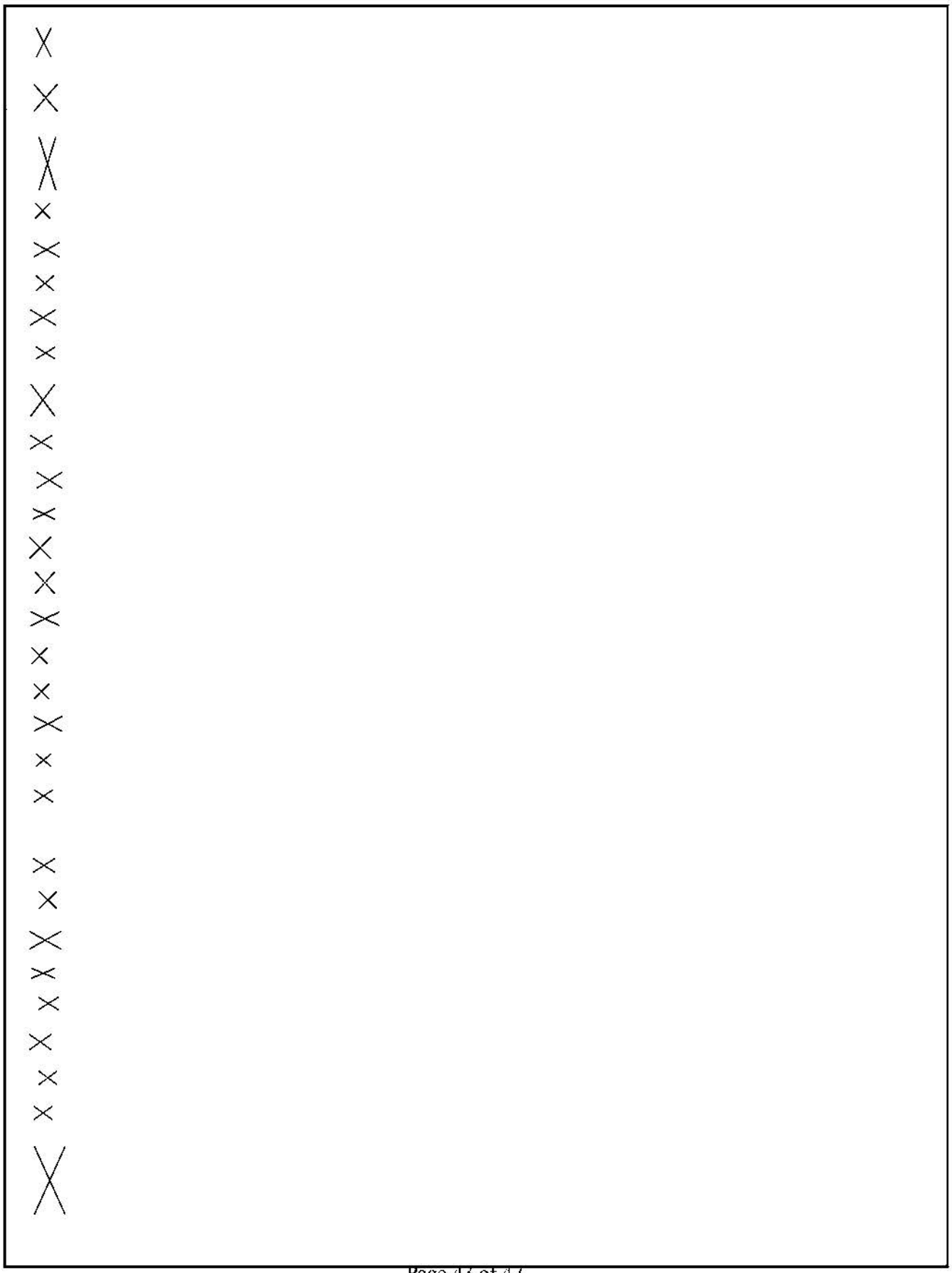
HRC-42

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

(U)



b3
b5
b6
b7C
b7E

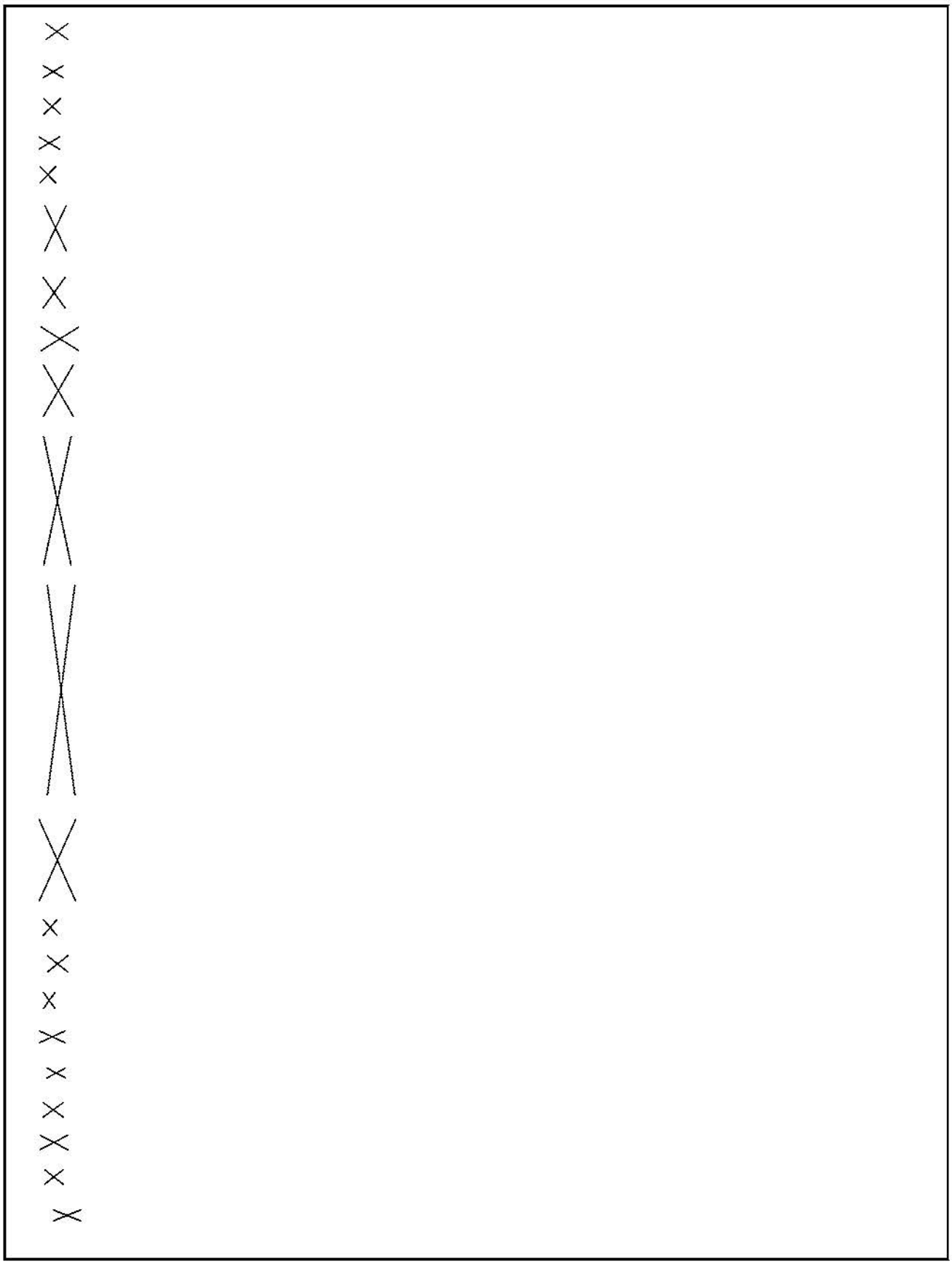
SECRET//ORCON/NOFORN

HRC-43

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E



b3
b5
b7E

SECRET//ORCON/NOFORN

HRC-44

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

(U)

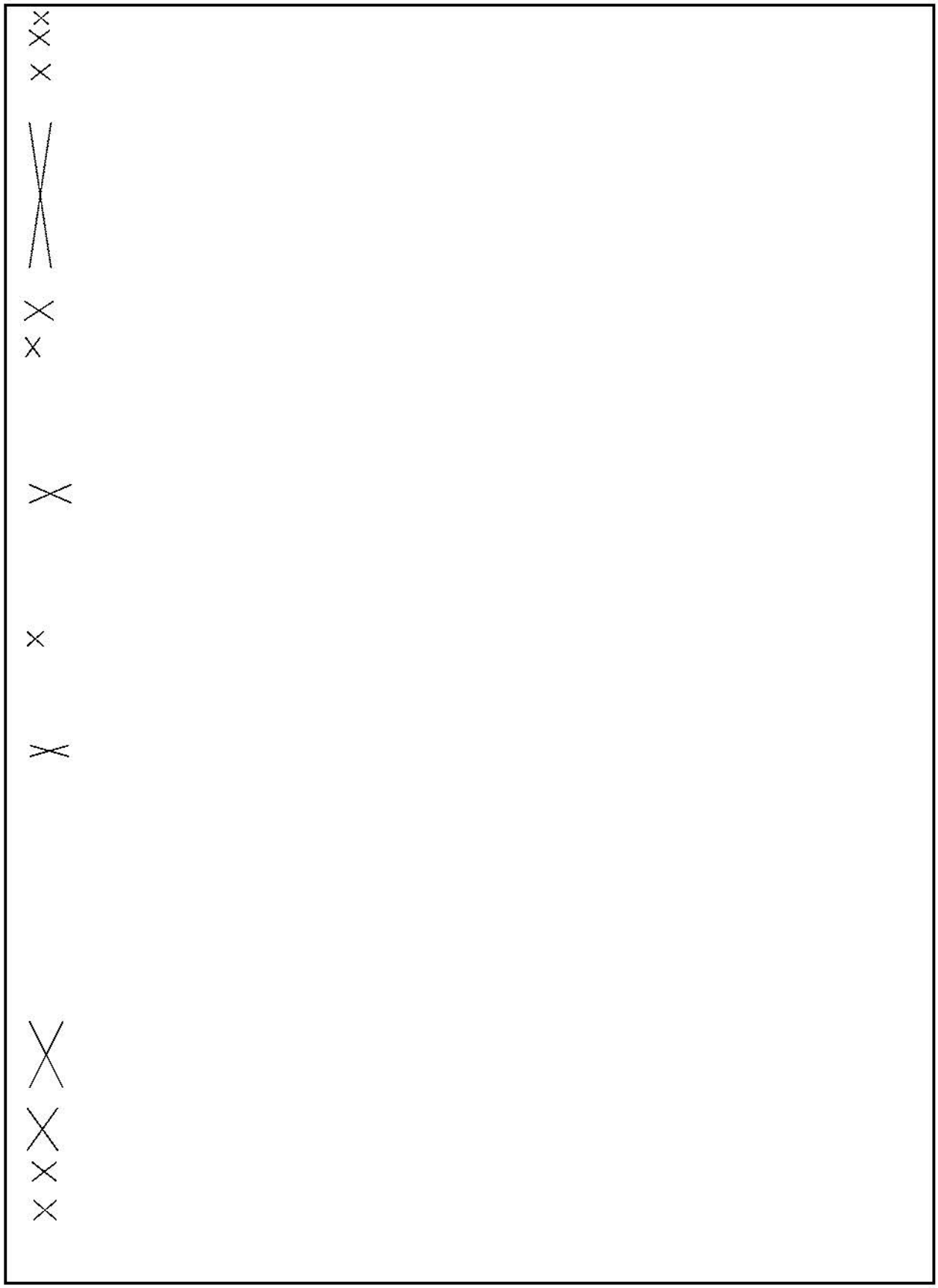
b3
b5
b6
b7C
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

SECRET//~~ORCON~~/NOFORN

b1
b3
b7E



b1
b3
b5
b6
b7C
b7E

SECRET//ORCON/NOFORN

HRC-46

b1
b3
b7E

SECRET//ORCON/NOFORN

b1
b3
b7E

b1
b3
b5
b7E

SECRET//ORCON/NOFORN

HRC-47

b1
b3
b7E