(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][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]

(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

[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]