surprised if classified information was being transmitted to Clinton's personal server.[510] [redacted] 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.

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.[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 [redacted] 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

b6
b7C

[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.