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

(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 t[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]

(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

[eeee] (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.