United States Senate

COMMITTEE ON
HOMELAND SECURITY AND GOVERNMENTAL AFFAIRS

WASHINGTON, DC 20510–6250

October 5, 2015

Mr. Victor Nappe
Chief Executive Officer
SECNAP Network Security Corp.
Technology Research Park
3651 FAU Boulevard, Suite 400
Boca Raton, FL 33431

Dear Mr. Nappe:

The Committee on Homeland Security and Governmental Affairs is examining former Secretary of State Hillary Clinton's use of a private email account and server during her time at the State Department. The Committee has obtained information confirming that a product offered by SECNAP Network Security Corp. (SECNAP)—CloudJacket SMB—was purchased to perform threat monitoring of the network connected to Secretary Clinton's private server in June 2013.[1] Within a period of nine months following CloudJacket's activation in October of 2013, SECNAP identified cyberattacks originating in countries such as China, the Republic of Korea, and Germany on Secretary Clinton's private server.[2] Further, the Committee has learned that from June 2013 to October 2013, it appears that the device was not active, raising concerns about whether the private server was vulnerable to intrusions.[3] The Committee is examining, among other things, the security of Secretary Clinton's server and network. I write to respectfully request your assistance with this important inquiry.

It was recently reported that Russian hackers attempted to access Secretary Clinton's email in 2011 through the use of an email-phishing scam.[4] Although the attack originating in Russia took place nearly two years prior to SECNAP's involvement in securing Secretary

---

[1] Email from Infograte to SECNAP Network Solutions (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

[2] Email from Infograte to SECNAP Network Solutions (June 26, 2013); *see also* Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (cyberattack allegedly originated from Internet Protocol (IP) address located in China); Email from SECNAP Network Security to Platte River Networks (Feb. 17, 2014) (cyberattack allegedly originated from IP address located in China); Email from SECNAP Network Security to Platte River Networks (March 4, 2014) (cyberattack allegedly originated from IP address located in "Korea, Republic of"); and Email from SECNAP Network Security to Platte River Networks (June 18, 2014) (cyberattack allegedly originated from IP address located in Germany) (all of the above emails are on file with the Committee on Homeland Security and Governmental Affairs).

[3] Email from Infograte to SECNAP Network Solutions (June 26, 2013); Email from SECNAP Network Security to Platte River Networks (Oct. 5, 2013) (confirming proper installation of CloudJacket for Secretary Clinton's private server) (both emails are on file with the Committee on Homeland Security and Governmental Affairs).

[4] Bradley Klapper, Jack Gillum, and Stephen Braun, *Russia-Linked Hackers Tried to Access Clinton Server, Emails Show*, ASSOCIATED PRESS (Sept. 30, 2015), *available at* http://abcnews.go.com/Politics/wireStory/6000-pages-clinton-emails-published-wednesday-34149824.

Clinton's private server, information received by the Committee suggests that cyberattacks originating in locations such as China, the Republic of Korea, and Germany occurred against the private server while SECNAP was monitoring threats to the network.[5] In one instance, the CloudJacket device discovered and automatically blocked malicious activity on the server.[6] According to one incident report, a SECNAP employee wrote that malicious activity based in "China was found running an attack against" Secretary Clinton's server.[7] While this specific attack was apparently detected and prevented, questions remain about whether the private server was vulnerable to cyberattacks prior to SECNAP's involvement, during the multi-month period between the purchase and activation of the CloudJacket device, and while the CloudJacket device was actively monitoring the server for malicious activity.

SECNAP delivers "unrivaled protection of network and information assets" using "next-generation information technology solutions that enable business to be conducted securely and privately on the Internet."[8] The CloudJacket device, like the one used on Secretary Clinton's network, is an intrusion prevention system that uses an "extensive and robust database of rules and signatures, and an expert experienced team of certified security engineers" to block network access to "even the most determined hackers."[9]

SECNAP provides two options for monitoring and supporting the CloudJacket device.[10] The first option is to pay a monthly fee for SECNAP Managed Service in which SECNAP expert Security Engineers will monitor the network around the clock. The second option is a "Do It Yourself Strategy" where the customer's own in-house staff monitors the network.[11] According to a document obtained by the Committee and titled, *CloudJacket Services Agreement*, it appears that Secretary Clinton's staff selected the first option, authorizing SECNAP to provide "real-time security incident response and forensics."[12]

---

[5] *See* Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (cyberattack allegedly originated from Internet Protocol (IP) address located in China); Email from SECNAP Network Security to Platte River Networks (Feb. 17, 2014) (cyberattack allegedly originated from IP address located in China); Email from SECNAP Network Security to Platte River Networks (March 4, 2014) (cyberattack allegedly originated from IP address located in "Korea, Republic of"); and Email from SECNAP Network Security to Platte River Networks (June 18, 2014) (cyberattack allegedly originated from IP address located in Germany) (all of the above emails are on file with the Committee on Homeland Security and Governmental Affairs).

[6] Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (on file with the Committee on Homeland Security and Governmental Affairs).

[7] *Id.*

[8] SECNAP Network Security Corp., Overview, http://www. secnap.com/overview/.

[9] SECNAP Network Security Corp., Patented Technology, https://www.secnap.com/products-services/cloudjacket/patented-technology/.

[10] SECNAP Network Security Corp., Managed Benefits, https://www.secnap.com/products-services/cloudjacket/managed-benefits/.

[11] *Id.*

[12] Contract between Clinton Executive Service Corp. (CESC) and SECNAP, CloudJacket Services Agreement (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

According to additional information received by the Committee, SECNAP entered into a contract with the Clinton Executive Services Corp. (CESC) on June 26, 2013.[13] According to documents, CESC oversaw contracting for the hardware, software, and security required for Secretary Clinton's private server and email.[14] However, the CloudJacket device that was intended to prevent malicious intrusions onto the network was not activated until October 5, 2013—three months after the device was purchased.[15] This gap raises questions about the vulnerability of Secretary Clinton's private server during the multi-month period that the CloudJacket device and management service was unable to monitor the network. During this period in which the CloudJacket device was inactive, a consultant for CESC recognized the potential security vulnerabilities and strongly urged CESC's leadership to approve a time for activation of the CloudJacket device. The consultant wrote:

> We really really [*sic*] need to do this and get you on board. We are left in a bad state. 1- We want to add in this extra security. We are paying for it and no[t] using the security. 2- we need to get you all fully on board[] so they can service you properly in case you have an issue.[16]

This apparent lack of security is concerning, particularly given the cyberattacks identified by SECNAP as soon as twelve days after the CloudJacket device was activated.[17]

In order to better understand SECNAP's role relating to Secretary Clinton's private server, the security capabilities of the private server, and any directives provided to SECNAP relating to security of the server, I ask that you please provide the following information and materials:

1. Please produce all documents and communications between or among employees or contractors of SECNAP and employees of Platte River Networks, Clinton Executive Services Corp. (CESC), the U.S. State Department, the U.S. Department of Justice, or any other entity referring or relating to Secretary Clinton's private server or network for the period January 1, 2009 to the present.

---

[13] Email from Infograte to SECNAP Network Solutions (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs). The contract between SECNAP and Clinton Executive Service Corp. (CESC) indicates a prepaid, 24-month fee and includes "real-time security incident response and forensics." *Id.* The contract appears to have been renewed in August 2015. *See* Email from CESC to Infograte (Aug. 19, 2015) (on file with the Committee on Homeland Security and Governmental Affairs).

[14] Email from Infograte to Platte River Networks (Apr. 16, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

[15] Email from Platte River Networks to Infograte (Sept. 27, 2013) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from SECNAP Network Security to Platte River Networks (Oct. 5, 2013) (confirming proper installation of CloudJacket for Secretary Clinton's private server).

[16] Email from CESC to Infograte (Aug. 19, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

[17] Email from SECNAP Network Security to Platte River Networks (Oct. 17, 2013) (unauthorized traffic was found scanning the network and was subsequently blocked) (on file with the Committee on Homeland Security and Governmental Affairs).

2. Please produce all contracts between SECNAP and Platte River Networks, CESC, the U.S. State Department, the U.S. Department of Justice, or any other entity referring or relating to Secretary Clinton's private server or network.

3. Please produce all invoices, bills, and receipts prepared by SECNAP or its representatives or agents regarding Secretary Clinton's private server and network.

4. Please produce all helpdesk, service, or support tickets generated by SECNAP related to Platte River Networks, CESC, or any other entity connected to the SECNAP services provided to secure Secretary Clinton's private server and network.

5. Please explain how CloudJacket secures a private server and network. If a private server is targeted by a cyberattack, how does CloudJacket identify the threat and notify SECNAP employees of a potential breach?

6. According to documents received by the Committee, SECNAP detected cyberattacks originating in China, Germany, and the Republic of Korea on Secretary Clinton's server or network.[18] Were there any other attacks from inside or outside of the U.S. directed at Secretary Clinton's server or network? If so, please identify the country where the attack originated from and whether the network or data was compromised.

7. Is SECNAP aware of any cyberattacks or breaches of Secretary Clinton's private server or network prior to its engagement to provide security services? Please explain.

8. After SECNAP's services were activated for Secretary Clinton's private server, did SECNAP identify any malicious material that was already installed on the private server? If so, please explain what steps SECNAP took to report and mitigate the issue.

9. According to documents received by the Committee, SECNAP was providing "24x7x365 monitoring and escalation of network intrusion alarms and events" for Secretary Clinton's private server and network.[19]

    a. During the time in which Secretary Clinton's private server was protected by CloudJacket, how many intrusion alarms and events were reported? Was the network or data ever compromised? Please explain.
    b. Does SECNAP's CloudJacket service maintain a log of intrusion alarms and events? If so, please provide the log to the Committee.

---

[18] Email from SECNAP Network Security to Platte River Networks (Feb. 8, 2014) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from SECNAP Network Security to Platte River Networks (Feb. 17, 2014) (on file with the Committee on Homeland Security and Governmental Affairs).
[19] Email from Infograte to SECNAP Network Security (June 26, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).

c. Please explain the process used by SECNAP to notify the managers of Secretary Clinton's private server and network about a network intrusion.
d. According to documents received by the Committee, there was a delay in activating the CloudJacket device.[20] After activation, how many days passed before CloudJacket identified the first network threat?

10. Please identify the employees at SECNAP who were responsible for providing services for Secretary Clinton's private server.

    a. According to documents received by the Committee, SECNAP employees are required to undergo background checks.[21] What level of investigation was undertaken during the background check process?
    b. Were any SECNAP employees cleared to access classified information? If so, what clearance levels did these employees possess?

11. According to publicly available information, SECNAP provides an email encryption service.[22] Did CESC purchase SECNAP's email encryption service? If not, did CESC indicate that encryption services were already in use?

Please provide this information and material as soon as possible, but no later than 5:00pm on October 19, 2015. Additionally, I ask that you please provide the Committee with a staff-level briefing to discuss SECNAP Network Solution's role in backing up the server.

The Committee on Homeland Security and Governmental Affairs is authorized by Rule XXV of the Standing Rules of the Senate to investigate "the efficiency, economy, and effectiveness of all agencies and departments of Government."[23] Additionally, S. Res. 73 (114th Congress) authorizes the Committee to examine "the efficiency and economy of operations of all branches and functions of the Government with particular reference to (i) the effectiveness of present national security methods, staffing and processes...."[24] For purposes of this request, please refer to the definitions and instructions in the enclosure.

---

[20] Email from Platte River Networks, to Infograte (Sept. 27, 2013) (on file with the Committee on Homeland Security and Governmental Affairs); *see also* Email from SECNAP Network Security, to Platte River Networks (Oct. 5, 2013) (confirming proper installation of CloudJacket for Secretary Clinton's private server).
[21] Email from Infograte to CESC (June 17, 2013) (on file with the Committee on Homeland Security and Governmental Affairs).
[22] SECNAP Network Security Corp., Email Encryption, https://www.secnap.com/products-services/spam-email-secuirty/email-encryption/.
[23] S. Rule XXV(k); *see also* S. Res. 445, 108th Cong. (2004).
[24] S. Res. 73 § 12, 114th Cong. (2015).

If you have any questions about this request, or concerns about the instructions or requirements in the enclosure, please contact [redacted] of the Committee staff at (202) 224-4751. Thank you for your prompt attention to this matter.

Sincerely,

Ron Johnson
Chairman

cc: The Honorable Thomas R. Carper
Ranking Member

Enclosure