U.S. Department of Homeland Security
UNITED STATES SECRET SERVICE

Washington, D.C. 20223

DIRECTOR

August 15, 2017

The Honorable Ted W. Lieu
U.S. House of Representatives
Washington, DC 20515

Dear Representative Lieu:

Thank you for your June 26, 2017 letter. Acting Secretary Duke asked that I respond on her behalf.

The Secret Service implements a range of programs and measures to ensure the security of the persons, facilities, and events we protect. The Secret Service partners closely in these efforts with both public and private organizations that may affect the security environment of our protectees. To ensure the security of key communications systems, the Secret Service closely partners with the White House Communications Agency and other interagency partners.

The Secret Service's Critical Systems Protection (CSP) program is one of the programs the Secret Service uses to mitigate potential security risks like those described in the May 17, 2017 Gizmodo report. The CSP program focuses on the protection of critical systems from cyber threats in support of the President, Vice President, and National Special Security Event (NSSE) venues. CSP assessments identify and assess computer networks, process-control systems or remotely controlled devices that could impact an operational security plan if compromised. The CSP program leverages the expertise of Secret Service special agents experienced in investigating network intrusions, and other significant cyber crimes, to ensure cyber risks do not impact our protectees. Owners and operators of computer systems have the foremost responsibility for securing their own systems; however, across both the Secret Service's investigative and protective activities, we have been highly successful at partnering with private organizations to implement appropriate and effective cybersecurity measures.

Brief answers to your five questions are enclosed; however, the capabilities and scope of these programs are inherently sensitive and therefore classified. We will gladly provide a classified brief regarding these programs to your office, upon your request. To schedule the briefing, please contact Special Agent in Charge Thomas Edwards by phone at 202-406-5676 or by email at: tcedwards@usss.dhs.gov.

Thank you again for your letter. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

RD Alles

Randolph D. Alles

Enclosure

The Department of Homeland Security's Response to Representative Lieu's June 26, 2017 Letter

1. **Is the Department of Homeland Security aware of the May 17th report in question?**

   The Department of Homeland Security is aware of the May 17, 2017 Gizmodo report. In addition to other potential security risks, the Secret Service routinely assesses and mitigates potential cybersecurity risks to Secret Service protectees, to include those related to the computer systems and locations discussed in the Gizmodo report.

2. **Are Secret Service staff who are responsible for cybersecurity familiar with the April 2017 DHS report entitled, "Study on Mobile Security," which details threats, vulnerabilities, and solutions to address identified weaknesses - and are they implementing DHS' recommendations on best practices?**

   The Secret Service contributed to the Department of Homeland Security Science & Technology report entitled, "Study on Mobile Security," and our cybersecurity staff has reviewed the final report and its recommendations on best practices. The Secret Service implements these and other security measures relevant to accomplishing our mission.

3. **Is any entity, public or private, responsible for securing Wi-Fi networks at properties belonging to the President - both while he is physically there, and when he is away - and if so, what entity is responsible?**

   The Secret Service assesses and mitigates a range of potential cybersecurity risks in order to ensure the security of protected persons, facilities, and events, including those security risks related to Wi-Fi networks. Our Critical Systems Protection (CSP) program assesses and mitigates the risk of a cyber-attack to critical systems and infrastructure that could affect the safety of agency protectees or could affect the implementation of our security plans while our protectees are onsite. Owners and operators of computer systems have the foremost responsibility for securing their own systems, to include Wi-Fi networks; however, the Secret Service has been highly successful at partnering with the owners and operators of critical systems to implement appropriate and effective cybersecurity measures, consistent with our protective responsibilities. The scope of Secret Service protective measures is inherently sensitive in nature, but we can arrange a classified briefing for you on CSP and related Secret Service programs.

4. **Although Secret Service routinely establishes portable and secure communications equipment, the President has reportedly held meetings in public spaces at his properties. Has Secret Service taken measures to ensure President Trump does not connect his personal mobile device to insecure networks while visiting his family's properties?**

   The White House Communications Agency (WHCA) and its partners take substantial steps to ensure the security of the President and his communication systems. The Secret Service collaborates with WHCA to address protective measures within the agency's purview.

The Secret Service countermeasure capabilities are inherently sensitive in nature. A classified briefing can be arranged for you on relevant agency programs.

5. **What measures has DHS and/or U.S. Secret Service taken to address the increased presence of unsecured digital devices - for example, Internet of Things-connected devices - in close proximity to the President?**

   The Secret Service has implemented a number of measures to address the risk associated with unsecured digital devices, to include "Internet of Things" devices. Often this involves simply disconnecting such devices for specific periods of time. The scope of Secret Service protective measures is inherently sensitive in nature, but we can arrange a classified briefing for you on relevant Secret Service programs.