United States Senate
WASHINGTON, DC 20510

January 17, 2019

The Honorable Kirstjen M. Nielsen
Secretary
U.S. Department of Homeland Security
2801 Nebraska Avenue, NW
Washington, D.C. 20528

Dear Secretary Nielsen:

We write to request additional information about how the Department of Homeland Security (DHS) is preparing law enforcement officials to effectively access and analyze digital evidence in support of criminal investigations.

While traditional evidentiary sources and methods remain critically important for prosecutions of criminal cases at the local, state, and federal levels, law enforcement officials increasingly must rely on digital evidence—including mobile communications devices, social media accounts, internet browsing histories, and myriad other data sources—to generate leads, identify suspects, and build and prosecute cases. Yet, as the Center for Strategic and International Studies (CSIS) recently reported, law enforcement agencies are facing significant challenges impeding their ability to effectively access and use digital evidence to support criminal investigations.[i] Central among these challenges is insufficient training and technical support to help law enforcement understand how legally to identify, handle, access, and analyze such evidence—a problem more far-reaching than accessing encrypted devices or data.

The CSIS report found that nearly one-third of law enforcement professionals cited difficulties in identifying which service providers had access to digital evidence as their largest challenge, followed by difficulties in obtaining evidence from providers, and a lack of resources needed to access and analyze data from devices.[ii] A 2018 study sponsored by the Bureau of Justice Assistance similarly found that "needs related to facilitating better communication and understanding between law enforcement and service providers" and "better investigator access to information and training on requesting remote digital evidence" ranked high among law enforcement's challenges.[iii]

As the need to use digital evidence grows and access to the myriad types of digital information available to law enforcement agencies becomes more technically complex, stronger coordination and more effective training for law enforcement personnel will prove invaluable, especially as access to and use of certain digital evidence raise issues of privacy or due process.

We share a commitment to ensuring U.S. law enforcement personnel are equipped with the best tools and training necessary to leverage digital evidence in their investigations. As such, we seek your assistance in providing information about how your department is working to combat these challenges. The Federal Law Enforcement Training Centers (FLETC) is the nation's largest

provider of law enforcement training, including training on digital evidence issues such as its Basic Incident Response to Digital Evidence course. In addition, other DHS entities, such as the Secret Service and the Immigration and Customs Enforcement, provide digital evidence training.

It would be useful to gain a deeper understanding of how you coordinate the training these entities provide with other involved federal agencies to ensure they meet the needs of the broader law enforcement community.

Accordingly, we would appreciate your responses to the following questions by no later than February 4, 2019:

1. What digital evidence training programs are provided by agencies or components of the Department? What legal authorities and budgetary accounts support each program?
2. What mechanisms do you have in place to coordinate relevant curricula and training platforms, both within your department and with other federal government agencies? How can the department better coordinate curricula and training platforms for digital evidence training across the federal government?
3. How is funding for these programs allocated at the local, state and federal levels? Are current programs adequate to meet the needs of the law enforcement communities they serve?
4. Please provide data about the personnel trained to better access and utilize digital evidence through these programs. How many law enforcement personnel are trained annually? What is the distribution of these training geographically, and across federal, state, and local levels?
5. What metrics are used for evaluating the success of these training programs?
6. What curricula and training platforms are currently in place to ensure local, state and federal law enforcement are, in their pursuit of digital evidence, not engaging in any conduct or actions which violate constitutional protections of privacy or due process? If such curricula and training platforms are not in place, what steps can the department take to incorporate such training into currently provided services?

Thank you for your consideration of this matter. We look forward to your response.

Sincerely,

BRIAN SCHATZ
United States Senator

THOM TILLIS
United States Senator

[i] William A. Carter, Jennifer Daskal, and William Crumpler, "Low-Hanging Fruit: Evidence-based Solutions to the Digital Evidence Challenge," Center for Strategic & International Studies, 25 July 2018, https://www.csis.org/analysis/low-hanging-fruit-evidence-based-solutions-digital-evidence-challenge.

[ii] Ibid.

[iii] Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson, "Identifying Law Enforcement Needs for Access to Digital Evidence in Remote Data Centers," Priority Criminal Justice Needs Initiative, 2018, https://www.rand.org/content/dam/rand/pubs/research_reports/RR2200/RR2240/RAND_RR2240.pdf.