

**Prehearing Questions for David James Glawe upon his nomination to be
The Under Secretary for Intelligence and Analysis
Department of Homeland Security**

Senator Wyden

- 1.) On February 20, 2017, I sent a letter to the Department of Homeland Security (DHS) with questions related to border searches of personal electronic devices of US persons. The Department responded on May 9, 2017. In my letter, I asked what legal authority permitted Customs and Border Protection (CBP) to ask for or demand, as a condition of entry, that US persons disclose their social media or email account passwords. DHS's May 9, 2017, letter stated that:

A person claiming to be a US citizen or lawful permanent resident must establish that fact to the inspecting officer's satisfaction (8 C.F.R. § 235.1(b) & (f)(1)(i)). In addition, an applicant for admission has the burden of establishing admissibility under the immigration laws (See 8 C.F.R. § 235.1(f)). If an applicant for admission is unable to establish admissibility, he or she may be denied admission. CBP has the authority to inspect and examine all individuals and merchandise entering or departing the United States, including all types of personal property such as electronic devices. (See, e.g., 8 U.S.C. § 1357; 19 U.S.C. § 1461, 1499; see also 19 C.F.R. § 162.6, stating that "[a]ll persons, baggage, and merchandise arriving in the Customs territory of the United States from places outside thereof are liable to inspection and search by a Customs officer").

- a. 8 U.S.C. § 1357(c) authorizes a search without warrant of the "personal effects in the possession of any person seeking admission to the United States" if the officer "may have reasonable cause to suspect that grounds exist for denial of admission to the United States under this Chapter which would be disclosed by such search." Is it DHS' interpretation of its authorities that it may only demand disclosure of a social media or email account password if there is reasonable cause to suspect that access to such accounts will provide grounds to deny admission? If so, how would DHS establish and document such reasonable cause?

In my prior capacity at CBP, I was not engaged in border search authority policy formulation or execution. I defer to the officials and attorneys at CBP and DHS for additional insight and information on this topic.

- b. 19 U.S.C. § 1461 and 19 U.S.C. § 1499 relate to imported goods. How would the contents of an email or social media account, with data stored on a U.S. server by a U.S. technology company, be considered an imported good?

I defer to the officials and attorneys at CBP and DHS for additional insight and information on the interpretation of 19 U.S.C. related to electronic media storage.

- 2.) **What statutory authorities allow CBP to request or demand that a U.S. person provide his or her personal electronic device PIN or password?**

In my prior capacity at CBP, I was not engaged in border search authority policy formulation or execution. I defer to the officials and attorneys at CBP and the DHS for additional insight and information on this topic.

- 3.) **DHS's May 9, 2017 letter stated that "CBP may request the traveler's assistance in presenting his or her effects – including electronic devices – in a condition that allows inspection of the item and its contents" (emphasis added). To the extent that the inspection of the "contents" of a personal electronic device requires the consent of the U.S. person traveler, is CBP required to first inform the traveler that he or she has the right to refuse to disclose a social media or email account password or device PIN or password?**

In my prior capacity at CBP, I was not engaged in border search authority policy formulation or execution. I defer to the officials and attorneys at CBP and DHS for additional insight and information on this topic.

- 4.) **Accessing a social media account likely involves accessing data not contained on the device, or physically within a functional area of the border. What statutory authorities allow CBP to search cloud data if a U.S. person does not provide CBP with consent to search their data?**

In my prior capacity at CBP, I was not engaged in border search authority or execution issues. I defer to the officials and attorneys at CBP and DHS for additional insight and information on this topic.

- 5.) **My February 20, 2017, letter requested data on the number of times in each calendar year 2012-2016 that CBP personnel asked for or demanded, as a condition of entry, that a U.S. person disclose a smartphone or computer password, or otherwise provide access to a locked smartphone or computer. DHS's May 9, 2017, letter stated that CBP did not have data responsive to this request. How many times in each calendar year 2012-2016 did CBP personnel obtain such passwords or otherwise obtain such access to a locked smartphone or computer?**

I do not have access to data responsive to this request. I defer to the officials at CBP for additional insight and information on this topic.

- 6.) **My February 20, 2017, letter requested data on the number of times in each calendar year 2012-2016 that CBP personnel asked for or demanded, as a condition of entry, that a U.S. person disclose a social media email account password, or otherwise provide CBP personnel access to data stored in an online account. DHS's May 9, 2017, letter stated that CBP does not have data responsive to this request.**

How many times in each calendar year 2012-2016 did CBP personnel obtain such passwords or otherwise obtain such access to stored accounts?

I do not have access to data responsive to this request. I defer to the officials at CBP for additional insight and information on this topic.

- 7.) CBP personnel met with my staff on March 8, 2017, to discuss the issue of border searches. During that meeting, my staff was informed that, in addition to conducting electronic device searches as part of their own investigations, CBP personnel will, on occasion, conduct an electronic device search at the request of another government agency. How many times have such searches taken place during each of the last five years? Please provide statistics for each requesting agency, for each year.**

I do not have access to data responsive to this request. I defer to the officials at CBP for additional insight and information on this topic.

- 8.) In a January 2017 interview with NBC News, you stated that CBP has "confidential human sources we run which falls under me as the national program manager."**

- a. Please describe the mission of these confidential source operations and the authorities under which CBP conducts them.**

CBP has a broad and complex statutory mission to secure the United States border, prevent the entry of terrorists and weapons of terrorism, and facilitate lawful trade and travel. 6 U.S.C. § 211. CBP's Confidential Human Source (CHS) program seeks to utilize information from human sources to fulfill this statutory mission. The use of a CHS by designated, trained CBP officers/agents can contribute significantly to the agency's ability to interdict individuals or merchandise/contraband attempting to unlawfully enter or exit the United States, in furtherance of the security of the Nation, and the safety of the public and CBP personnel.

CBP operates its CHS program consistent with its statutory authorities including, but not limited to, those set forth in Titles 6, 8, 19, and 31 of the U.S. Code, as well as implementing regulations. If confirmed, I will work to assist you in getting the most up-to-date information about CBP CHS operations from CBP.

- b. Do these confidential human sources operate inside the United States? If so, please describe the coordination with FBI and the extent to which they are subject to Attorney General or other relevant guidelines.**

In all CBP CHS operations, CBP coordinates and de-conflicts with the FBI and other agencies as appropriate. CBP's Confidential Human Source Policy Manual sets forth CBP's policies and procedures regarding CHSs. This Policy Manual, issued in 2015, was modeled in part upon CHS guidelines promulgated by the

Department of Justice and other federal law enforcement agencies. If confirmed, I will work to assist you in getting the most up-to-date information about CBP CHS operations from CBP.

- c. **As the Chief Intelligence Officer of DHS (CINT), what would be your role in coordinating between CBP human source operations, or any other DHS human source operations, and the Intelligence Community?**

As the DHS CINT, I expect my role coordinating DHS Component Confidential Human Source operations would be similar to the CINT role coordinating other DHS Component intelligence capabilities: to exercise leadership and authority over the formulation and implementation of policy and programs throughout the Department, and to provide strategic oversight of and support to the intelligence-related missions and goals of the DHS Intelligence Enterprise. With respect to DHS Component Confidential Human Source programs, I would also focus on coordinating DHS activities with the rest of the IC agencies, and work to ensure that DHS activities are not duplicative of similar programs in place across the IC.

It is my understanding that the DHS CINT has no role coordinating or tasking directly DHS Component CHS operations. Given the fact that DHS collectively comprises the largest federal law enforcement presence in the United States, I feel that is a missed opportunity. Human enabled intelligence collection is a critical element of the intelligence collection cycle, and the information it yields is essential in identifying and unraveling criminal networks. I believe it is incumbent upon I&A, as the Department's representative to the IC, to facilitate opportunities for the DHS Intelligence Enterprise to collaborate with IC partners on Confidential Human Source operations to enhance coordination, reduce potential duplication, and add value to the overall homeland security mission. If confirmed, I look forward to reviewing this topic further and working with Congress and other stakeholders to find ways to further enhance the CINT's ability to fully exercise the authorities associated with the position.