June 20, 2017 Due Diligence Questions for Kevin McAleenan
Nominee for Commissioner of U.S. Customs and Border Protection (CBP)

Similar questions, with the exception of question 1(c), were sent to David J. Glawe, nominated to be Under Secretary for Intelligence and Analysis at the Department of Homeland Security, via Sen. Wyden's capacity on the SSCI.

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

   A person claiming to be a U.S. citizen or a 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 USC §1357(c) authorizes a search without a 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's 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?

      Thank you for these questions and for the opportunity to further address the issue of authorities in this important and sensitive area.

      In addition to long-standing precedent, including from the Supreme Court, that recognizes the broad scope of CBP's authority to conduct border searches,[1] this authority is enshrined in numerous statutes – which support

[1] CBP is authorized to conduct a border search of travelers, conveyances, and merchandise crossing the United States border. As the Supreme Court has long recognized, the border search doctrine operates as an exception to the warrant and probable cause requirements of the Fourth Amendment. *United States v. Flores-Montano*, 541 U.S. 149, 152-53 (2004) (quoting *United States v. Ramsey*, 431 U.S. 606, 616 (1977)) ("Time and again, [the Supreme Court has] stated that 'searches made at the border, pursuant to the longstanding right of the sovereign to protect itself by stopping and examining persons and property crossing into this country, are reasonable simply by virtue of the fact that they occur at the border.'"). Border searches may be performed at places such as the border (the

CBP not only in the enforcement of the nation's immigration laws, but also empowers CBP in support of our customs, agriculture, and counterterrorism missions at the border. Just as CBP is responsible for inspecting luggage, vehicles and cargo upon arrival to the United States, in this digital age CBP must also conduct limited and targeted inspections of electronic devices to determine whether they contain contraband (such as child pornography), information indicating inadmissibility, or information that could present a threat to national security (such as counterproliferation concerns).

While 8 U.S.C. § 1357(b) is an example of CBP's authority to conduct a search in the immigration context, CBP concurrently operates under a host of additional statutory authorities that more broadly provide that all persons, baggage, and merchandise arriving in, or departing from, the United States are subject to inspection, search, and detention. *See, e.g.*, 19 U.S.C. §§ 1461; 1496; 1499. Those statutory Customs authorities are applicable to all travelers entering the United States, regardless of their citizenship.

On this point, because CBP must determine the admissibility of both the traveler and his or her accompanying goods and baggage, even after a returning U.S. citizen has established his or her identity and U.S. citizenship, CBP may conduct a border search of the goods he or she is seeking to bring into the country to ensure that those goods are permitted to enter. In other words, because *any* traveler may be carrying an electronic device that contains evidence relating to offenses such as terrorism, illegal smuggling, or child pornography, CBP's authority to search such a device at the border does not depend on the citizenship of the traveler.

In the exceedingly rare instances when CBP seeks to conduct a border search of information in an electronic device[2] – which affects less than one-hundredth of one percent of travelers arriving to the United States – CBP will never prevent a U.S. citizen from entering the United States because of a need to inspect that traveler's device. Therefore, although CBP may detain an arriving traveler's electronic device for further examination, in the

---

territorial boundaries of the United States that exist on land, sea, and air) or the functional equivalent of the border (e.g., the airport where an international flight to the United States lands). Border searches of electronic devices do not require a warrant or suspicion, except that following the decision in *Cotterman v. United States*, 709 F.3d 952 (9th Cir. 2013), certain searches undertaken in the Ninth Circuit require reasonable suspicion of activities in violation of a law enforced or administered by CBP.

[2] CBP exercises this authority very judiciously and has made available to the public, since 2009, its governing policy on the border search of information in electronic devices. Although CBP's law enforcement policy directives are generally issued internally for official use only, CBP recognized the importance of the public dialogue on this issue, and CBP Directive No. 3340-049, *Border Search of Electronic Devices Containing Information*, includes comprehensive guidance for searching, reviewing, retaining, and sharing information obtained from border searches of electronic devices containing information. It remains publicly available at: https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf. For your reference, I have attached a copy of that directive to this response.

limited circumstances when that is appropriate, CBP will not prevent a traveler who is confirmed to be a U.S. citizen from entering the country because of a need to conduct that additional examination.

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?

CBP's authority to conduct border searches extends to all merchandise entering or departing the United States, including information that is physically resident on an electronic device transported by an international traveler. Therefore, border searches conducted by CBP do not extend to information that is located solely on remote servers. I appreciate the opportunity to offer that clarification.

c. Does CBP make a distinction between viewing data that is on a foreign platform, and perhaps stored on foreign servers, versus domestic platforms and servers? If so, how would CBP know where the data is stored?

In conducting a border search, CBP does not access information found only on remote servers through an electronic device presented for examination, regardless of whether those servers are located abroad or domestically. Instead, border searches of electronic devices apply to information that is physically resident on the device during a CBP inspection.

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?

As referenced in the response to question 1(a) above, CBP has the statutory authority to inspect and examine all travelers and merchandise entering or departing the United States, including personal property such as electronic devices. *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"). CBP may seek a traveler's assistance in presenting his or her merchandise – including electronic devices – in a condition that allows CBP to conduct a lawful search. This assistance may occur by CBP requesting that the traveler open the manual lock on his or her suitcase, or unlock or otherwise make accessible the traveler's accompanying electronic device, in order to permit an otherwise authorized border search of information that is physically resident on that device to proceed.

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?

As with any other aspect of the border search process, CBP's inspection of an electronic device transported by an international traveler does not require the consent of that traveler. To the extent that a CBP officer decided to conduct a border search on a traveler's goods or merchandise that was locked, or was otherwise not immediately available for inspection, the officer can request the traveler's assistance in opening or presenting the goods. If CBP is unable to determine whether an item is admissible in the condition as presented by the traveler, CBP may choose to detain the item pending a determination of its admissibility in accordance with the law.

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?

As explained in greater detail above, CBP border searches extend to the information that is physically resident on the device, and does not extend to information that is solely located on remote servers (known as solely "in the cloud"). In fact, with my concurrence, CBP's Office of Field Operations issued a nationwide muster in April 2017 reminding its officers of this precise aspect of CBP's border search policy. For your convenience, I have attached a copy of that muster to this response. As you will see, that muster is marked for official use only and contains law enforcement sensitive information.

Questions 5-6:

5. Senator Wyden's 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?

6. Senator Wyden's February 20, 2017 letter requested data on the number of times in each calendar year 2012–2106 that CBP personnel asked for or demanded, as a condition of entry, that a U.S. person disclose a social media or 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?

DHS's prior responses on these points are correct, and CBP does not maintain data responsive to these particular requests.

However, as the questions seek information about border encounters that conditioned entry on a traveler providing a password, it is important to understand that CBP does not condition entry of U.S. citizens based on provision of a password, and has not denied entry into the United States to any U.S. citizen because of a refusal by such person to provide a password that would unlock their accompanying electronic device. Information that may be identified during a border search of an electronic device is just one piece of the totality of the circumstances involved in CBP's decision-making during a border inspection, and CBP will not prevent a traveler who is confirmed to be a U.S. citizen from entering the country because of a need to conduct that additional examination.

7. CBP personnel met with Senator Wyden's staff on March 8, 2017 to discuss the issue of border searches. During that meeting, Wyden 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.

DHS's prior response on this point is correct. However, CBP's policy on how it coordinates with other federal agencies when it seeks to conduct a border search of information in electronic devices is described in detail in Directive 3340-049, which is available at https://www.dhs.gov/xlibrary/assets/cbp_directive_3340-049.pdf and attached hereto. In particular, section 5.3.2 of that directive describes the circumstances when CBP could seek assistance from another federal agency to conduct a border search of information in an electronic device (for technical assistance or subject-matter assistance) and the limitations under which that assistance could be provided. CBP is assessing whether further data collection can assist in administering the careful use of this authority in the future.