Senator Rand Paul
Post-Hearing Questions for the Record
Submitted to Kirstjen M. Nielsen

Nomination of Kirstjen M. Nielsen to be Secretary of the Department of Homeland Security
Wednesday, November 8, 2017

1. At the U.S.-Mexico and U.S.-Canada border, DHS personnel have used the so-called border search exception to conduct searches of Americans within 100 miles of a border, without a warrant or even probable cause. These searches are premised on individuals transiting to or from the United States, yet many millions of Americans live and work in these zones and are not transiting into or out of the country. The result is that Americans in large swaths of the country have diminished constitutional rights.
   - Question: Should the regulations on which this practice is based be updated to more narrowly define this practice?
   - Question: Do you believe any geographic limitation exists to where and how DHS personnel may deploy suspicionless checkpoints within the United States?

In response to both questions above:

Customs officers are 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. Border searches may be performed at places such as the border (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).

Immigration checkpoints concern separate authority. More specifically, the Immigration and Nationality Act (INA) § 287(a)(3) authorizes law enforcement agents to board and search for aliens on vessels located in U.S. territorial waters and vehicles or conveyances located within a reasonable distance from the exterior boundary of the United States. A "reasonable distance" under this statute extends 100 air miles inland from the border of the United States. Additionally, when making a stop pursuant to INA § 287(a)(3) at locations other than an immigration checkpoint, an agent must have at least reasonable suspicion to stop a vehicle. Any search of the vehicle will have to be separately justified via consent to search, or probable cause to conduct a readily mobile conveyance search of the vehicle. DHS does not conduct suspicionless checkpoint searches.

- Question: If confirmed as Secretary, will you expand the use of suspicionless checkpoints within the United States?

  If confirmed, I will work to ensure that DHS will adhere to all applicable legal authority and judicial decisions concerning checkpoint operations. DHS does not conduct suspicionless checkpoint searches.

  I understand that the Department's Office for Civil Rights and Civil Liberties (CRCL) recently investigated allegations related to the checkpoints and found that CBP checkpoints were not violating the constitutional rights of persons transiting. However, CRCL is working with CBP to enhance public outreach and CBP training to ensure that travelers and agents are aware of their rights when crossing at checkpoints.

- Question: Do you support the capture of all vehicle information by DHS, including license plates, for vehicles that travel through a DHS checkpoint—including those that have done nothing wrong and are simply driving from Point A to Point B as part of their daily business? If so, what limitations on this practice—including storage of vehicle information—might you support?

  As I understand it, U.S. Border Patrol checkpoints utilize license plate reader (LPR) technology for the purpose of identifying illegal alien smuggling. LPR technology is utilized at checkpoint locations that have been identified as routes of travel utilized by alien smugglers. Checkpoints and LPR technology further assist the overall national security mission.

  Currently CBP captures the data and maintains it for seventy-five years, and the images for two years (due to storage limits), as stipulated in the TECS System of Record Notice.

  If confirmed, I will work with CBP, DHS Counsel, and CRCL to ensure that the constitutional rights of all Americans are upheld with respect to vehicle information emanating from a DHS checkpoint.

2. I remain concerned about reported instances of American citizens being detained at points of entry when traveling back into the United States—in particular, the reported instances of Americans being asked by DHS officials to turn over their phones or other digital devices for search, including:
   i. This year, a NASA engineer and U.S. citizen was reportedly pulled into inspection when returning from a vacation in Chile. The individual subjected to inspection recounted how Customs and Border Protection (CBP) demanded the PIN to his phone and handed him a form that

explained how CBP had the right to copy the contents of his phone. He recalled that the form indicated that participation in the search was "mandatory" and it threatened "detention and/or seizure" of the device if he did not comply.[1] He was reportedly released after providing the PIN to his phone—a work phone that was itself property of NASA.[2]

ii. Two U.S. citizens were stopped on a return from Canada and held for two hours after their phones were taken by CBP officers. They alleged that they were stopped again on another return trip from Canada three days later in which they were again told to turn over their phones. They also alleged that CBP officers physically took one of the phones in order to search it.[3]

iii. An NBC News investigation reported that they examined 25 different cases of U.S. citizens being told to turn over their phones, unlock them, or provide passwords to CBP officers.[4]

iv. A U.S. citizen was reportedly stopped from boarding a flight in Los Angeles, handcuffed, and released after "a Homeland Security agent looked through his phone for about 15 minutes."[5]

v. In 2015, a U.S. citizen journalist alleged that, while traveling back to Texas from Brazil, he was detained while officials "went through all his contacts, emails and WhatsApp messages on his phone."[6]

- Question: If DHS agents lack a warrant, would you as Secretary allow an American citizen, a green card holder, or any other valid visa holder to be delayed or denied entry into the United States if the individual refuses to provide his device's password, unlock his device, or otherwise provide access to the information on his device? If yes, under what authority, and how does an individual's citizenship or visa status affect your answer?

The Secretary of Department of Homeland Security is under an obligation to safeguard our country to the extent possible by law. Legal issues such as this

---

[1] https://www.theatlantic.com/technology/archive/2017/02/a-nasa-engineer-is-required-to-unlock-his-phone-at-the-border/516489/

[2] http://www.cnn.com/2017/02/13/us/citizen-nasa-engineer-detained-at-border-trnd/

[3] http://www.nbcnews.com/news/us-news/american-citizens-u-s-border-agents-can-search-your-cellphone-n732746

[4] ibid

[5] https://www.nytimes.com/2017/02/14/business/border-enforcement-airport-phones.html

[6] https://www.buzzfeed.com/tasneemnashrulla/this-american-journalist-said-he-was-detained-at-miami-airpo?utm_term=.elMvKx0EB#.goOwWgBpZ

will be determined with the assistance of counsel provided by the DHS Office of General Counsel. I would asked to be further briefed on this if confirmed. However, as I understand the current law, all persons and their devices arriving in the US are subject to a border search because CBP must determine the admissibility of both the traveler and his or her accompanying goods and baggage, to ensure that those goods are permitted to enter. In other words, and as I understand it, 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.

Importantly, I also understand that 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 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. CBP's public guidance to travelers I think succinctly summarizes current policy and practice. (https://www.cbp.gov/sites/default/files/documents/inspection-electronic-devices-tearsheet.pdf).

To be clear, I believe that all CBP officers are and should be required to strictly adhere to all constitutional and statutory requirements and CBP has strict oversight policies and procedures that implement these safeguards. To my knowledge, the instances in which CBP seeks to conduct a border search of information in an electronic device are exceedingly rare – I remember the statistic that such searches affect less than one-hundredth of one percent of travelers arriving to the United State.

- Question: If you believe you have the authority to delay entry in any of these instances, what is the maximum amount of time you believe you can delay entry for each an American citizen, a green card holder, or any other valid visa holder?

  CBP exercises border search 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, 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 on the DHS website. ICE, which also has border search authority, issued a companion policy directive on this topic at the same time as CBP.

I understand that CBP's policy specifically states that CBP will protect the right of individuals against unreasonable search and seizure and will ensure privacy protections. To that end, it recognizes that, if a border search of an electronic device cannot be completed during the time that the traveler is at the port of entry, the device may be detained by CBP, ordinarily for a period not to exceed five days, after the traveler has departed the port of entry. Therefore, additional time needed to complete a thorough border search will not necessarily require the traveler to remain at the port of entry during the time of the search.

Moving forward, and in recognition of the requirement described in law, which require CBP to review and update at least every three years its standard operating procedures relating to searches of electronic devices at ports of entry, I understand CBP is currently reviewing the CBP Directive and intends to revise and update it to reflect evolving operational practices on this important and sensitive issue. If confirmed, I will ensure that such revision and update complies with all laws, protects Constitutional rights, and provides sufficient information to the reader about border searches of electronic devices.

- Question: As Secretary, would you permit the sharing of information gathered at the border from electronic devices with other federal, state, and local law enforcement?

As I understand it, CBP's governing policy directive specifically recognizes the potential need to share information with other federal agencies in order to seek their assistance and expertise to enable CBP to complete the border search. Further, any information shared occurs in accordance with the governing Privacy Act system of records notice.

- Question: On June 6, 2017, General John Kelly told me that "we don't [search phones] routinely unless there's a reason why…we do it whether they're citizens or non-citizens coming in." This is a change from what he told me on April 5, 2017, when he said "I just don't believe we're doing it." As Secretary, will you continue his policy of searching the contents of phones at the border?

If confirmed, I will work to ensure that CBP, and all of DHS complies with all laws, regulations and court cases in executing its mission. Currently, as I understand it, in addition to long-standing precedent, including that of the Supreme Court, that recognizes the broad scope of CBP's authority to conduct border searches, this authority is enshrined in numerous statutes – which support 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. It is my understanding that given today's threats and the CBP mission, similar to CBP's responsibility 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 WMD information).

- Question: You have indicated informally, and your predecessor as Secretary has indicated, that you do not detain U.S. citizens if they refuse to submit their digital devices to an electronic search at a point of entry. However, in such a scenario, would you seize or otherwise seek to separate the U.S. citizen from their device? Would you ask the U.S. citizen to leave the point of entry while agency officials retain possession of the device(s)? Does DHS assert that it has the authority, regardless of whether it is current practice, to separate a U.S. citizen from their digital device(s) at a point of entry for the purposes of an electronic search? If so, what procedures govern such actions?

As I understand it, there are CBP Directives on point. Specifically, one that recognizes that in the rare instance an international traveler's cell phone or other electronic device may need to be detained (beyond the time that the traveler is at the port of entry) to complete the necessary border search, there is a specified process for such a detention, including the requirement that a traveler receive a custody receipt and that the traveler be notified of the search when such a fact can be disclosed without hampering national security or law enforcement or other operational considerations.

In addition, the Directive provides that searches of electronic devices should be conducted in the presence of the traveler unless there are national security, law enforcement, or other operational considerations that make it inappropriate to permit the individual to remain present.

3. If confirmed, what will you do to ensure employees can and will disclose violations of law, rule, or regulation, and instances of fraud, waste, abuse and mismanagement within the DHS to any or all appropriate sources, including Congress?

I will work to foster an environment of respect and trust, providing ways in which voices can be heard and engaging with employees at various levels to identify and address concerns. I have always been a person who speaks truth even when the truth is uncomfortable. If confirmed, I will encourage the same candor from all DHS employees, and expect that managers will also foster an environment of trust and respect and will listen to any employee concerns and take actions to address them. Overall, we must foster a culture at the Department that encourages the same "see something, say something" attitude of vigilance we promote to the public and safeguard those who do come forward in compliance with whistleblower laws and regulations. I believe all DHS employees have a duty to report all such violations you describe. If confirmed, I will uphold all legal protections for the reporting of fraud, waste, abuse and mismanagement within DHS, and, in my position, will be especially vigilant to the issue of any potential management retaliation. I will partner with the IG to ensure that all complaints are properly investigated. I will also ensure that employees understand and have ready access to information describing the various ways to disclose violations of law, rule or regulation, and instances of fraud, waste, abuse and mismanagement within DHS.

4. Notwithstanding the recent cancellation of some $16 billion of the program's debt by Congress, the National Flood Insurance Program will remain deeply in the red for the foreseeable future. The Office of Management and Budget, in its Oct. 4, 2017, disaster supplemental request to Congress, called the NFIP "simply not fiscally sustainable in its current form."[7]
    - Question: Do you support any of the proposed reforms that OMB included in its Oct. 4 supplemental request? If yes, which proposed reforms? If no, what NFIP reforms would you support?

Yes. I strongly support reforms to the NFIP. As the Administration and many in Congress have noted, the program is not sustainable. Reforms are necessary such as those to enable a robust private market and to raise rates to reflect risk while including a means tested affordability program.

---

7 https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/Letters/Letter%20regarding%20additional%20funding%20and%20reforms%20to%20address%20impacts%20of%20recent%20natural%20disasters.pdf

5. As "the only [Intelligence Community] element statutorily charged with delivering intelligence to state, local, tribal, territorial and private sector partners,"[8] the DHS Office of Intelligence and Analysis presents potential dangers to civil liberties, including a blurring of the line between domestic law enforcement and intelligence gathering activities as well as intentional abuse or inadvertent misuse of intelligence products.
    - Question: If confirmed, what will you do to insure that any and all intelligence gathered or disseminated by DHS will be handled with utmost concern regarding people's privacy and other rights by all entities that may receive or encounter such information?

      As I remember from my time as Chief of Staff, DHS has extensive mechanisms in place to guard against the concerns you have described, including built-in oversight within the Office of Intelligence and Analysis and safeguards through the Office of Privacy, the Office of Civil Rights and Civil Liberties, the Office of the General Counsel, and appropriate inspectors general. If confirmed, I commit to ensuring that DHS remains focused on gathering and disseminating intelligence information strictly within the confines of the law and with utmost respect for privacy, civil rights, and civil liberties.

    - Question: With regard to Fusion Centers, what will you do to ensure the appropriate use of and consistent privacy protections for information shared by them among their partner entities?

      While fusion centers are owned and operated by state and major urban area governments, as I understand it, to the extent they receive federal grants, access to federal networks, and DHS personnel, they are also subject to thorough oversight and review to ensure they comply with all relevant laws and have rigorous policies in place to respect privacy, civil rights, and civil liberties. If confirmed, I will work with the Department's Under Secretary for Intelligence and Analysis to review DHS policies and procedures with regard to fusion centers to ensure they continue to handle information appropriately and to make sure any and all DHS personnel assigned to those centers are in compliance with requirements and have the necessary training to protect sensitive information, individual privacy and other rights.

[8] https://www.dhs.gov/office-intelligence-and-analysis

6. From your tenure as DHS Chief of Staff, what ideas and aspirations do you have to improve the management of the Department of Homeland Security with respect to identifying and eliminating waste, fraud or abuse?

As described above, I will work to foster an environment of respect and trust, providing ways in which voices can be heard and engaging with employees at various levels to identify and address concerns. I have always been a person who speaks truth even when the truth is uncomfortable. If confirmed, I will encourage the same candor from all DHS employees, and expect that managers will also foster an environment of trust and respect and will listen to any employee concerns and take actions to address them. I believe all DHS employees have a duty to report instances of fraud, waste or abuse. Overall, we must foster a culture at the Department that encourages the same "see something, say something" attitude of vigilance we promote to the public and safeguard those who do come forward in compliance with whistleblower laws and regulations. If confirmed, I would review the various options available for reporting fraud, waste or abuse and ensure that such options are accessible to all DHS employees. I will also ensure that employees understand and have ready access to information describing the various ways to disclose instances of fraud, waste, or abuse within DHS, to include reporting to the IG and GAO.

If confirmed, I will uphold all legal protections for the reporting of fraud, waste, or and mismanagement within DHS, and, in my position, will be especially vigilant to the issue of any potential management retaliation. I will partner with the IG to ensure that all complaints are properly investigated and that if a process doesn't exist today, that one is created to track reporting, investigate claims and ensure needed revisions or adjustments are made my managers and leadership. Should there be any gaps in authorities to appropriately address any of the concerns raised, I will work with the Congress.

Finally, as was discussed in a recent IG report, we must strengthen the DHS internal control environment to ensure that the Department can effectively, efficiently and lawfully execute its mission. If confirmed, I will work with the Deputy Secretary and the Under Secretary for Management to expand and strengthen our internal controls.

7. As your nomination moves forward, will you commit to providing a written response to any further questions related to your nomination prior to your confirmation vote?

Yes.