QUESTIONS FOR THE RECORD
MR. DAVID J. GLAWE

QUESTIONS FOR THE RECORD FROM SENATOR KING

1. **In response to the Committee's prehearing questions, you stated that all DHS I&A analytic products must follow "ICD 203 tradecraft standards." If confirmed, what steps will you take to ensure these standards for analytic integrity are strictly adhered to?**

   It is my understanding that the Office of Intelligence and Analysis' (I&A) Planning, Production, and Standards Division (PPSD) evaluates all I&A products for compliance with the nine tradecraft standards laid out in ICD 203 as well as a tenth developed specifically by I&A to ensure maximum coordination and collaboration with Intelligence Community (IC) and DHS Intelligence Enterprise (DHS IE). If confirmed, I would ensure I&A analysts receive adequate and continuing training on each of these standards. I would also ensure tradecraft quality reviews are built into the production process at both the beginning and near the end of the process, ensuring tradecraft subject matter experts have ample opportunity to conduct initial reviews as well as final evaluations. The final evaluations are critical to ensure finished products adhere to tradecraft standards. They can also be used to capture best practices and common mistakes that can be incorporated into training on the front end.

2. **What do you consider the appropriate role of intelligence to be in the formulation of policy? Is it appropriate to draft an intelligence product with the specific intent of supporting an administration policy, either legally or politically, in mind?**

   In my view, it is never appropriate to produce intelligence with the specific intent of supporting a pre-conceived policy position. It is appropriate to provide policymakers with timely, accurate, objective, and integrated intelligence and information to inform policy decisions. When intelligence information needed by policymakers is not available, it is also appropriate to work with those policymakers and other elements of the IC to close those gaps. If confirmed, I would strive to provide intelligence and information

without regard to political positions or influence.

3. What avenues of redress are available to you in the event you are pressured to politicize intelligence? If confirmed, would you access those avenues of redress if asked to compromise your professional obligation to oversee and lead the production of objective and politically unbiased intelligence analysis? Do you consider this Committee to be among those avenues of redress?

If confirmed, I would strive to provide intelligence and information without regard to political positions or influence. If I ever felt pressured to produce intelligence in support of a pre-conceived policy position or politicize intelligence in any way, I would not hesitate to avail myself of the most appropriate avenue of redress. I consider DHS leadership, the Director of National Intelligence, and the Inspectors General of DHS and of the IC as my primary avenues of redress. Depending on the source and extent of the concern, I would also consider the Committee as another avenue of redress.

4. Do you support allowing the Government Accountability Office's (GAO) cleared auditors access to DHS I&A for conducting classified audits and reviews at the request of this Committee?

Yes. It is my understanding that I&A has been a cooperative partner of GAO, and has benefited from the GAO's work.

5. The 2016 "Hack the Pentagon" pilot program and subsequent Department of Defense "bug bounty" programs have helped identify vulnerabilities within the Department's information systems. In your view, what role should such bug bounty programs play in our government's cyber-security strategy?

In the area of cybersecurity, the role of the Under Secretary for Intelligence and Analysis at the Department of Homeland Security is to produce intelligence and share information in support of the Department's cybersecurity mission. I have reviewed open source information regarding the "Hack the Pentagon" pilot program. To the extent they could help the Department identify previously unknown network vulnerabilities or further define intelligence requirements, I believe "bug bounty" programs could be useful tools within a larger government-wide cybersecurity strategy.

QUESTIONS FOR THE RECORD FROM SENATOR WYDEN

Signaling System 7

In April 2017, the Department of Homeland Security (DHS) issued a Study on Mobile Device Security. The report concluded that vulnerabilities in Signaling System 7 (SS7) could be used to determine the physical location of phones, disrupt phone service, and intercept or eavesdrop on communications. According to the report, DHS "believes that all U.S. carriers are vulnerable to [SS7] exploits, resulting in risks to national security, the economy, and the Federal Government's ability to reliably execute national essential functions." Further, these "vulnerabilities can be exploited by criminals, terrorists, and nation-state actors/foreign intelligence organizations."

6. Do you agree with the assessments in the report?

Yes.

7. How significant is the counterintelligence threat posed by the SS7 vulnerabilities?

I am not in a position to offer an informed assessment of the significance of the counterintelligence threat related to SS7 vulnerabilities. However, I understand I&A's Counterintelligence Division is in close contact with IC partners on this topic. If confirmed, I will endeavor to learn more about potential counterintelligence threats posed by these vulnerabilities and ensure the DHS Counterintelligence Program is positioned to identify and mitigate any counterintelligence threats directed at DHS employees or systems related to these vulnerabilities.

8. What is the role of the Office of Intelligence and Analysis in ensuring that SS7 vulnerabilities and similar threats identified by the Science and Technology Directorate or other components of the Department are brought to the attention of counterintelligence elements of the Intelligence Community?

I&A provides intelligence support to the Department's cybersecurity

and critical infrastructure protection missions. If confirmed, I will work to ensure I&A's Counterintelligence Division coordinates closely with IC partners to assess threats related to the vulnerabilities identified in this report and share intelligence about those threats with customers. The Under Secretary for Intelligence and Analysis also serves as the Department's Counterintelligence Executive, so I would also work to ensure the DHS Counterintelligence Program is positioned to identify and mitigate any counterintelligence threats directed at DHS employees or systems related to these vulnerabilities.

9. What steps do you believe the Department should take to warn federal agencies and employees of those agencies whose mobile phones may be vulnerable as a result of SS7 vulnerabilities?

I believe DHS has a duty to warn and collaborate with federal and industry partners to implement an effective mitigation strategy which minimizes vulnerabilities identified in the report. If confirmed, I will work with my DHS colleagues at the Science and Technology (S&T) and National Protection and Programs Directorates (NPPD) to ensure they have the intelligence support they need to develop and implement effective mitigation measures.

10. Will you commit to ensuring that my staff is provided a briefing on SS7 vulnerabilities and actions being taken by the Department to address them?

It is my understanding that DHS S&T, who led DHS efforts on this report, provided your staff with a briefing on this topic on July 7, 2017, and that DHS NPPD is also in contact with your staff about arranging a follow-up briefing. If confirmed, I would work to ensure I&A is positioned to support any future briefings, if necessary.

Stingrays

Multiple press stories have described the capability of cell site simulators, sometimes called IMSI catchers or "stingrays," to track mobile phones and intercept communications (e.g., "Tech firm tries to pull back curtain on surveillance efforts in Washington, *The Washington Post*, September 17, 2014;

"Someone is spying on cellphones in the nation's capital, *CBC News*, April 3, 2017).

11. Do you agree that the placement of illicit "stingray" devices, particularly around government buildings in Washington, D.C., would pose a serious counterintelligence concern?

I am not in a position to offer an informed assessment of counterintelligence threats related to cell site simulator technology. If confirmed, I will work to ensure I&A's Counterintelligence Division coordinates closely with IC partners to assess counterintelligence threats associated with these technologies. The Under Secretary for Intelligence and Analysis also serves as the Department's Counterintelligence Executive, so I would also work to ensure the DHS Counterintelligence Program is positioned to identify and mitigate any counterintelligence threats directed at DHS employees or systems related to these technologies.

12. Is the Department of Homeland Security seeking to locate any illicit stingrays in Washington, D.C.?

I am not aware of any DHS effort to locate illicit cell site simulator technology devices in Washington, D.C.

Clandestine Human Collection

In responses to pre-hearing questions, you wrote "[a]s the DHS [Chief Intelligence Officer], I expect my role coordinating DHS Component Confidential Human Source [CHS] 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 for the DHS Intelligence Enterprise… 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."

13. Under what legal authority could the DHS CINT coordinate or task DHS Component CHS operations?

I understand the role of the CINT includes providing strategic oversight of DHS Component intelligence activities and establishing intelligence collection, processing, analysis, and dissemination priorities and policies for the DHS Intelligence Enterprise. As stated above, I do not believe the DHS CINT has an independent authority to directly task DHS Component Confidential Human Source (CHS) operations.

14. How would the tasking, by an entity of the Intelligence Community of non-IC collectors, be covered under Executive Order 12333 and other relevant authorities?

It is my understanding that in general, it is within the DNI's enumerated authorities to provide "advisory tasking" to non-IC establishments consistent with Attorney General approved procedures specific to that activity. I am not aware of such procedures ever having been established, nor do I have any specific knowledge of how this process may have been used. With regard to DHS, I do not believe the CINT has an independent authority to directly task DHS Components. To the extent any such authority were to be established for the DHS CINT, I assume that authority would most likely derive from the authorities of the DHS Secretary, and not from those of the DNI, Executive Order 12333, or any other IC authority.

GAO Report on Confidential Informants

In your responses to pre-hearing questions, you wrote that "[Customs and Border Protection'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." In September 2015, GAO issued a report entitled "Confidential Informants; Updates to Policy and Additional Guidance Would Improve Oversight by DOJ and DHS Agencies" (GAO 15-807), which reviewed the policies and processes that apply to CBP, Immigration and Customs Enforcement (ICE), the U.S. Coast Guard (USCG), and the U.S. Secret Service (USSS). The report stated that the relevant Attorney General Guidelines do not explicitly apply to DHS agencies and that neither the Guidelines nor DHS requires a review of DHS component agencies' policies.

15. What is your view of the findings of the GAO report?

I believe the findings were valuable, and as the lead for CBP's Confidential Human Source (CHS) program, I ensured the recommendations were incorporated into that program. It is my understanding that CBP's CHS program is fully compliant with DOJ CHS policy and guidelines, and that CBP has implemented GAO's recommendations.

16. In response to one of GAO's Recommendations for Executive Action, "DHS concurred with our recommendation that DHS provide oversight and guidance to ensure that DHS agencies comply with the Guidelines. DHS stated that it plans to designate a DHS entity to be responsible for developing, implementing, and overseeing policies and programs to ensure DHS-wide compliance with the Guidelines, as appropriate." What is your understanding of DHS's implementation of this recommendation?

While I was not involved in DHS's implementation of this recommendation, I have reviewed information on GAO's website related to this recommendation. It is my understanding that DHS issued a policy guidance memo on the use of confidential informants in July 2016. GAO found that policy guidance memo consistent with their recommendation. They agreed it would help ensure component agencies take action to update their policies consistent with the Guidelines, and they consider this recommendation closed.

17. In response to another one of GAO's Recommendations for Executive Action, "DHS concurred with our recommendation that ICE and USCG update their respective policies and corresponding monitoring processes. DHS stated that ICE will review requirements related to the oversight of informants' illegal activities as part of an ongoing update to its informant handbook. DHS stated that USCG has issued an interim policy that requires compliance with Guidelines and that USCG also plans to do a comprehensive review and revision of its policy." What is your understanding of DHS's implementation of this recommendation?

While I was not involved in DHS's implementation of this recommendation, I have reviewed information on GAO's website related

to this recommendation. It is my understanding that both USCG and ICE have taken steps to address this recommendation. USCG issued an updated confidential informant policy, and GAO found that policy consistent with their recommendation. ICE is in the process of updating its relevant policy handbooks and expects to implement them by December 2017.

QUESTIONS FOR THE RECORD FROM SENATOR HARRIS

A CNN story from February 25, 2017 titled, "White House effort to justify travel ban causes growing concern for some intelligence officials" alleges that, "some DHS officials are concerned that the new I&A director—Acting Undersecretary for Intelligence David Glawe—may be politicizing intelligence" and references your role in preventing a report from moving forward. The referenced report may have reached conclusions that were inconsistent with the White House's policy position.

18. During the hearing, we discussed your involvement with the intelligence report related to the travel ban. Let me be clear of your answer: did you delay the release of this intelligence report? If yes, why?

Thank you for the opportunity to clarify. I did not delay the release of the document cited in the CNN article. The document went through the standard coordination processes, but due to the evolving situation with the Executive Order, it was never finalized. Apart from reviewing a draft of the document at the time of coordination, I played no further role in the document's production or disposition.

There was a related but separate I&A intelligence assessment that I did have a more active role in reviewing at approximately the same timeframe. The assessment, initiated by I&A in August 2016, focused on foreign-born, US-based violent extremists that conducted or attempted to conduct terrorist activity in the United States. It was prepared and coordinated through standard processes and briefed to I&A and DHS leadership prior to its finalization and dissemination. When I received the draft assessment and briefing, I was concerned that it did not include information from ongoing law enforcement cases, nor did it cover individuals who were tried or removed from the United States for reasons other than terrorism charges. Given the nature of the topic and the scope of the draft document, I directed the authors to seek additional information from relevant federal law enforcement agencies for incorporation into the product, and official coordination from IC members with access to such information. Although the information was not made available to I&A analysts, I&A published and disseminated the report with official coordination from an IC partner. The report included an expanded scope

note to describe what sources of information were and were not included in assessment, and no significant changes were made to the findings. I felt it was important to seek this coordination and concurrence from IC partners to protect the integrity of I&A's analytic tradecraft and ensure the document's findings were accurate and backed by to the original source documents and "raw" intelligence.

19. During your time as Acting Under Secretary of DHS, were you ever pressured to alter intelligence conclusions to support White House policy?

No.

20. Do you believe that citizenship is a reliable terrorist threat indicator?

I believe that to fully assess the threats posed by terrorist organizations, it is important to evaluate not only the operators executing the attack, but also the origins of the individuals, their support networks, and the locations from which these support networks operate.

21. In your opinion is it appropriate for DHS I&A to be tasked to create an intelligence product that supports a policy position of the administration?

In my view, it is never appropriate to produce intelligence with the specific intent of supporting a pre-conceived policy position. It is appropriate to provide policymakers with timely, accurate, objective, and integrated intelligence and information to inform policy decisions. When intelligence information needed by policymakers is not available, it is also appropriate to work with those policymakers and other elements of the IC to close those gaps. If confirmed, I would strive to provide intelligence and information without regard to political positions or influence.

22. In your opinion, is it appropriate for an intelligence product to be produced for purposes of supporting litigation related to an Administration policy?

In my view, it is never appropriate to produce intelligence with the

specific intent of supporting a pre-conceived policy position. It is appropriate to provide policymakers with timely, accurate, objective, and integrated intelligence and information to inform policy decisions. In some circumstances, I believe it may be appropriate to cite intelligence information or products in litigation and judicial proceedings. For example, original sources of intelligence and associated products are routinely used in the Foreign Intelligence Surveillance Court proceedings. However, it is critical that such information not be produced with the specific intent of supporting a pre-conceived policy position.

23. In your words, how do you see the importance of analytic objectivity for members the intelligence community, including DHS I&A?

Analytic objectivity is the foundation of sound analytic tradecraft and is critical in maintaining the integrity of analysis. If confirmed, I would strive to provide intelligence and information without regard to political positions or influence.

24. What is your understanding of the current mechanisms or channels within DHS I&A to raise analytic dissent?

It is my understanding that I&A utilizes a variety of mechanisms to resolve both internal and external dissent that may arise due to differences of opinion regarding the analytic line of a specific product.

Internally, analysts meet informally to discuss and resolve differences of opinion as a product is being drafted. If the dissent emerges from a senior analyst, manager, or other leadership, the parties can meet with the analytic ombudsman to determine the cause of the dissention and help identify a path forward. If the ombudsman process proves unsuccessful, the Inspector General should be notified to determine whether an investigation is warranted. In addition, external parties such as agency leadership or congressional oversight committees could be contacted to review and address the issue.

If dissent arises externally across agencies, I&A can use several mechanisms to resolve the dissent. The first and most important is for analysts to discuss and address concerns during the coordination

process while drafting the product. If unable to resolve at their level, analysts should report the issue to the senior analysts and managers to resolve during the draft phase. If differences of opinion remain, the dissenting agency has a responsibility to formally outline its position and an alternative analysis for inclusion in the final product. If that dissent is rejected by the product's author, the dissenting agency can then appeal to the ODNI's Office of Analytic Standards for review or engagement with the IC's analytic ombudsman.

25. If confirmed, will you support and if necessary expand upon these mechanisms?

Yes.

26. If confirmed, will you commit to resist any attempts by the White House, or anyone else, to politicize DHS's intelligence analysis?

Yes.

27. If confirmed, will you commit to notify this Committee of any attempts by the White House, or anyone else, to politicize DHS's intelligence analysis?

Yes.