(b)(3)

The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek our cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber “hygiene” scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State

to offer assistance, share information, and provide additional resources to state and local officials.

Background Questions

What activities related to the US election does the USIC attribute to Russia?

- The IC has high confidence in its attribution of the intrusions into the DNC and DCCC, based on the forensic evidence identified by a private cyber-firm and the IC's own review and understanding of cyber activities by the Russian Government.

What about the disclosures that occurred after the DNC and DCCC intrusions?

- At least some of the disclosures, including the disclosures of DNC and DCCC documents by Guccifer 2.0, DCLeaks, and others from June to August 2016, are consistent with the methods and motivations of Russian-directed efforts.

- The disclosures by DCLeaks and Guccifer 2.0 are consistent with the information stolen from the DNC and DCCC, thus suggesting Moscow is at least providing the information or is possibly directly responsible for the leaks.

- The disclosure of White House e-mails by DCLeaks also appears to be consistent with tactics and motivations of the Russian Government.

- Similarly, the disclosures of medical information from the World Anti-Doping Agency by a hacker group calling itself "Fancy Bear" are consistent with the cyber tactics and motivations of the Russian Government.

How did the US IC attribute the DNC and DCCC intrusions to the Russian Government?

- The IC independently observed technical activity that is consistent with the forensic evidence identified by a private cyber-firm and is consistent with our general understanding of cyber activities by the Russian Government.

Does the USIC believe additional Russian action to interfere with our elections is imminent?

- We expect that Russia will continue its efforts up to Election Day.

Has the USIC concluded that Russia is behind the "Shadow Brokers" disclosures?

- We are not in a position to comment on Shadow Brokers at this time.

Was Hal Martin, the recently arrested former NSA contractor, part of this Russia-sponsored effort?

- We are not able to comment on ongoing criminal investigations, so we would refer you to the Department of Justice.

Do you assess that Putin ordered these operations?

- We believe that authorization to conduct these operations could only have come from the most senior levels of the Russian Government.

Has the US concluded that Russia is responsible for the intrusions into state election systems?

- We are not definitively attributing the intrusions into state elections systems to the Russian Government, but the fact that they are consistent with Russian motivations and intent behind the DNC and DCCC intrusions, suggests Russian involvement.

Is Russia trying to alter the outcome of the US election?

- The Kremlin probably expects that publicity surrounding the disclosures will raise questions about the integrity of the election process and would undermine the legitimacy of the President-elect.

What is the USG doing about this?

- The American public and our democracy are resilient to foreign attempts to manipulate public opinion. The U.S. Government is committed to ensuring a secure election process and has robust capabilities to detect efforts to interfere with our elections.

- The President has made it clear that we will take action to protect our interests, including in cyberspace, and we will do so at a time and place of our choosing. Consistent with the practice we have adopted in the past, the public should not assume that they will necessarily know what actions have been taken or what actions we will take.

What options are you considering for your response?

- We are not going to discuss potential responses except to say that as we implement our responses, some responses you may see, and others you may not.

Why is the USG publicly attributing these actions now? Why didn't the USG attribute this sooner?

- Determining attribution is a complex process. As the IC gathered new information, it was able to reach higher degrees of confidence about which actors are responsible and then determine what could be disclosed publicly, while appropriately protecting sources and methods.

The U.S. Government does not make attribution determinations very often. Does this mean you have changed your position on attribution?

- Determining attribution is a complex process. As the IC gathered new information, it was able to reach higher degrees of confidence about which actors are responsible and then determine what could be disclosed publicly, while appropriately protecting sources and methods.

- Publicly identifying those actors is a step that the government considers when we have confidence in the attribution and can make the information public, consistent with U.S. national security interests, including the protection of sources and methods, and when doing so advances U.S. national interests.

What is DHS doing to help state and local governments raise their cybersecurity protections ahead of the elections?

- DHS is providing several services to state and local election officials to assist in their cybersecurity. These include cyber "hygiene" scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and addressing potential cyber threats. As of October 6, more than half of the states have contacted DHS and are in discussions about receiving one or more of these services.

- DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting voting infrastructure and the elections process.

- Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share information, and provide additional resources to state and local officials.

Why hasn't DHS designated the election system to be a critical infrastructure sector?

- At this point, we do not believe that designating election systems as a critical infrastructure sector would provide significant new authorities or resources to safeguard these systems in the near term. We have committed that we will not take any action on this issue until after the election and we have had sufficient opportunity to consult with the states. Right now, our priority is to help state officials ensure the security of their systems. In the longer term, we want to work with state officials to help them understand

the practical benefits of being designated as critical infrastructure and to seek their input on whether or not designation is appropriate.

What is included in or meant by election infrastructure?

- While there is no generally accepted definition of election infrastructure, DHS understands this term as the collection of systems and processes, administered by state and local governments, used to conduct elections. This collection includes information technology systems to register voters, maintain and disseminate accurate rolls of registered voters, create and disseminate ballots, enable voters to cast ballots, and accurately count and report on cast ballots in a timely manner. It covers all modes of voting, including in-person, early, absentee, vote-by-mail, and Internet voting.

Who is responsible for the systems?

- The responsibility for administering these systems varies widely by jurisdiction, but typically resides with the Secretary of State or Governor.

What is DHS doing to secure voting infrastructure?

- DHS is providing risk assessments and conducting hygiene scans, and has deployed cybersecurity advisors and protective security advisors throughout the country to provide support to state election officials. The DHS National Cybersecurity and Communications Integration Center serves as a 24x7 incident response center and can provide on-site assistance to identify and remediate a cyber incident.

- In addition to the work already being done by states and the operational cybersecurity support being provided through the National Protection & Programs Directorate, DHS stood up an Election Infrastructure Cybersecurity Working Group with experts from all levels of government to raise awareness of cybersecurity risks potentially affecting voting infrastructure and promote the security and resilience of the electoral process.

Given these revelations, do you still have confidence in the U.S. electoral system?

- Yes, we remain confident in the integrity of the U.S. election system for several reasons:
    - The diverse and diffuse nature of our voting infrastructure makes it very difficult to manipulate the outcome of an election.
    - States ensure that voting machines are not connected to the Internet.
    - There are numerous checks and balances as well as extensive oversight at multiple levels built into our electoral process.

Since you have not designated the election infrastructure as a critical infrastructure sector, does that mean it is not important or that you will not take steps to defend it?

- Free and fair elections are a hallmark of our democracy, and we would consider any action that interferes with the right of Americans to participate in our election process as an attack on our democratic way of life.
- Regardless of whether the election infrastructure is designed as a critical infrastructure sector, we will take all necessary steps to sustain the integrity of our elections.
- The primary responsibility for protecting our election infrastructure resides with the states and local governments that administer elections, and that's the way it should be. However, the Federal government, and DHS in particular, stands ready to assist states and local governments if they request it.

Has Congress been consulted regarding this incident?

- Congress is regularly briefed about significant cyber threats and other intelligence reporting concerning the numerous and expanding range of malicious cyber actors threatening the United States and its interests around the world.

- Consistent with this practice, appropriate Congressional leadership were informed about these incidents, and we intend to continue to update them on the incident as the situation warrants.