QUESTIONS FOR THE RECORD

Dr. Samuel Liles, Acting Director of Cyber Division, Office of Intelligence and Analysis

And

Jeanette Manfra, Acting Director of Undersecretary, National Protection and Programs Directorate

U.S. Department of Homeland Security

QUESTIONS FOR THE RECORD FROM SENATOR WARNER

1. **Question: Please provide a description of the full scope of Russian attempts to interfere in the 2016 elections in the United States by hacking into, or attempting to hack into state and local election systems, including, but not limited to, voter registration databases, voting machines, voting-related computer networks or secretaries of state and other election officials' networks.**

   Response: The Office of Intelligence and Analysis (I&A) published a comprehensive intelligence report in early October 2016, largely based on suspected malicious tactics and infrastructure, that cataloged suspicious activity we observed directed at state government election infrastructure across the country. While not a definitive source in identifying individual activity attributed to Russian government cyber actors, it established that Internet-connected election-related networks, including websites, in 21 states were potentially targeted by Russian government cyber actors. A copy of this product has been previously provided to this committee.

   This cyber activity was characterized by similarities in the tactics employed, the infrastructure used by malicious cyber actors, and the victimized networks themselves. The activity was also, concurrent with the Russian government's compromise and leaks of e-mails from U.S. political figures and institutions. The capabilities and tactics were largely in the form of spear-phishing individual e-mail accounts and attempts to exploit database vulnerabilities using Structure Query Language (SQL) injection.

   Supported by classified reporting we've refined our understanding of individual targeted networks, but the scale and scope noted in that October 2016 report still generally characterizes our observations: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

2. **Please identify the 21 states potentially targeted by Russian government cyber actors referenced in the prepared testimony and provide any additional relevant information related to localities and the nature of the targeted networks.**

Response: While not a definitive source in identifying individual activity attributed to Russian government cyber actors, the Department of Homeland Security (DHS) is aware of Internet-connected election-related networks, including websites, in at least 21 states that were potentially targeted by Russian government cyber actors. Although we've refined our understanding of individual targeted networks, supported by classified reporting, our observations include: a small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

Entities impacted by malicious cyber activity engage with the Department of Homeland Security on a voluntary basis. Our success requires strong partnerships built on trust and confidentiality. By identifying affected entities, we not only make it less likely that the affected entity will continue to engage with DHS, but also it becomes less likely that other entities are willing to share information with the government.

It's important to note, however, that by working with affected entities, the Department has been able to share information with thousands of election officials about the nature of the threat. Facing the threat of cyber-enabled operations by a foreign government during the 2016 elections, the Department of Homeland Security conducted unprecedented outreach and provided cybersecurity assistance to state and local election officials. Through numerous efforts before and after Election Day, DHS and our interagency partners have declassified and publicly shared significant information related to the Russian malicious cyber activity. These steps have been critical to protecting our elections, enhancing awareness among election officials, and educating the American public.

QUESTIONS FOR THE RECORD FROM SENATOR WYDEN

3. **According to the January 2017 Intelligence Community Assessment (ICA), DHS assessed that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying." DHS's prepared testimony stated that it is "likely that cyber manipulation of U.S. election systems intended to change the outcome of a national election would be detected."**

   What level of confidence does DHS have in its assessment included in the ICA?

   Response: DHS I&A has moderate confidence in the ICA that "the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying," a judgement based on our analysis of observed Russian cyber operations, the Intelligence Community's ability to detect such activity, and the Department's insight into the various components of U.S. election infrastructure.

4. **Does DHS assess that it would be likely that cyber manipulation of U.S. election systems intended to change the outcome of a state or local election would be detected?**

   Response: Beyond our separate assessment of the access Russia developed into U.S. election infrastructure in 2016- accesses that did not provide the direct ability to alter vote tallies - DHS I&A has high confidence that it is likely that cyber manipulation of US election infrastructure intended to change the outcome of a national election would be detected. We have not made an assessment of state-wide or local elections.

   Does DHS assess that it would be likely that cyber manipulation of U.S. election systems would be detected, regardless of whether it was intended to, or did, change the outcome of any U.S. election?

   Response: Multiple checks and redundancies in U.S. election infrastructure—including diversity of systems, non-Internet connected voting machines, pre-election testing, and processes for media, campaign, and election officials to check, audit, and validate results—make it likely that cyber manipulation of U.S. election systems, at a scale and scope intended to change the outcome of a national election, would be detected. There is always the possibility that individual or isolated cyber intrusions into U.S. election infrastructure could go undetected, especially at local levels, but a broad coordinated effort is likely to be detected.

5. **To what extent does the ability to detect cyber manipulation of vote tallying depend on whether the manipulation is conducted through remote access of internet-connected systems or through other means?**

   Response: The risk to U.S. computer-enabled election infrastructure varies from county to county, between types of devices used, and among processes used by polling stations. These factors, among others, introduce resilience in the overall system but also introduce numerous variables into our ability to detect cyber manipulation of U.S. election infrastructure, whether remotely or through physical access to a system. We judge that physical access to a system, in most cases, would be more difficult to detect than remote access, but an accurate assessment of our ability to detect an individual cyber intrusion into U.S. election infrastructure is system-specific, especially against vote tallying systems that are diverse and generally non-Internet connected.

6. **DHS's prepared testimony describes a range of services available to state and local election officials. Do these services address possible vulnerabilities related to vote tallying systems, particularly systems that are not internet-facing? If not, why not? If so, to what extent did state and local election officials avail themselves of these services?**

Response: The Department of Homeland Security (DHS) has shared information with election officials, including indicators of compromise, technical data, and best practices that assist officials with addressing threats and vulnerabilities related to election infrastructure that is not Internet-facing.

Additionally, DHS offers risk and vulnerability assessments. These assessments are more thorough and done on-site by DHS cybersecurity experts. They typically require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When DHS conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. Due to available resources, these assessments are available on a limited basis.

Generally, DHS is authorized, upon request, to provide cybersecurity functions including technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may include attribution, mitigation, and remediation. As we continue to work with election officials, we may identify opportunities to provide additional services.

7. **DHS testimony during the hearing included the following: "We are currently engaged with many vendors of [voting machine] systems to look into conducting some joint forensics with them. The vendor community is very interested in engaging with us.... Our department has not conducted forensics on specific voting machines."**

   What is the timeline for conducting joint DHS-vendor forensic examinations of voting machines?

   How broadly will those examinations be conducted? In what states will they be conducted and what percentage of voting machines will be subject to the examinations?

   What is the role of state and local election officials in this effort?

   Response: The Department of Homeland Security (DHS) continues to work with the vendor community to determine what cybersecurity services would be of interest to them, to include vulnerability testing. DHS's work with vendors and election officials is on a voluntary basis. To the extent that technical assistance is requested from vendors and resources are available, DHS will leverage its capabilities to provide assistance.

8. **Has DHS conducted any assessments of the ability of state and local authorities, technology vendors and contractors to identify and defend against sophisticated cyber attacks conducted by nation states? If so, what are those assessments?**

   Response: On September 20, 2016, the Department of Homeland Security published an intelligence assessment on Cyber Threats and Vulnerabilities to US Election Infrastructure. The assessment was published at the unclassified-for official use only level. This assessment was shared with federal stakeholders and states' election officials.

9. **The Election Assistance Commission (EAC) issues voluntary voting system guidelines. How many states adhere to these guidelines?**

   Response: The Election Assistance Commission is an independent agency. Based on discussions with the Election Assistance Commission, we understand that there are at least 41 states that use Federal standards and certification processes in some manner. For more detailed information, we respectfully defer to the EAC.

10. **Does DHS have an assessment about the value of paper voting or the risks posed by paperless electronic voting systems? If so, what is that assessment?**

    Response: Owners and operators of critical infrastructure manage risk. The Department of Homeland Security (DHS) has prioritized efforts to assist state and local election officials address cybersecurity and physical risks related to election infrastructure. DHS has not made recommendations related to how a state should or should not allow voters to cast ballots.

11. **According to an investigation by Politico, Kennesaw State University, which is responsible for all voting technology for the state of Georgia, had lax cybersecurity, which security researchers exploited to download registration records for the state's 6.7 million voters and multiple PDFs with instructions and passwords for election workers to sign in to a central server on Election Day. The report also stated that the University failed to fully correct these vulnerabilities even after it was notified.**

    Does DHS concur with the findings of the investigation?

    What actions can be taken to address the vulnerabilities identified by the investigation and what role could DHS have played, or could play in the future in addressing those vulnerabilities?

    Response: The Department of Homeland Security (DHS) is authorized, upon request, to provide cybersecurity functions including technical assistance, risk management support, and incident response capabilities to Federal and non-Federal entities with respect to cyber threat indicators, defensive measures, cybersecurity risks, and incidents, which may

include attribution, mitigation, and remediation. DHS did not receive a request for assistance in relation to the facts described in this question. As a result, DHS did not conduct an independent assessment related to the findings of the investigation.

12. In August 2016, DHS announced it had created an Election Infrastructure Cybersecurity Working Group. Who is on this Working Group and does it include cybersecurity experts with a technology background?

Response: The Department has had significant engagement efforts with election infrastructure stakeholders since last year. The Election Infrastructure Cybersecurity Working Group announced in August 2016 included officials from the Department of Homeland Security, the Department of Justice, the Federal Bureau of Investigation, the National Institute of Standards and Technology, the National Association of Secretaries of State, The Election Assistance Commission, and the National Association of State Election Directors. This group was leveraged prior to the 2016 election to share information and consider options.

The Secretary formally established the Election Infrastructure Subsector in January 2017. As the Sector-Specific Agency the Department will provide overall coordination guidance on election infrastructure matters to subsector stakeholders. As part of this process, the establishment of the Election Infrastructure Subsector (EIS) Government Coordinating Council (GCC) is nearing completion. The EIS GCC will be a representative council with the mission of focusing on sector-specific strategies and planning. This will include development of information protocols and establishment of key working groups, among other priorities, once chartered and meeting regularly. As part of the GCC establishment, we recently assembled a cyber-focused Election Infrastructure Operational Working Group (OWG) comprised of key Federal, state and local partners. The purpose of the group is to jointly develop information sharing requirements and protocols using the expertise of key state election officials and the Multi-State Information Sharing Analysis Center (MS-ISAC). This OWG has membership from across the Department of Homeland Security's National Protection and Programs Directorate, Election Assistance Commission, National Association of Secretaries of State, National Association of State Election Directors, key county officials, and the MS-ISAC. The OWG includes many cybersecurity experts with technology backgrounds and will continue to refine requirements as it matures.

13. To what extent should secretaries of state and other election officials receive security clearances necessary to obtain cyber threat information from the federal government?

What level of clearance is required?

Response: The Department of Homeland Security is committed to providing security clearances to state chief election officials and select election support personnel, on a "need to know" basis. While the predominance of information sharing will be at the unclassified level, working with cleared election officials allows the sharing of relevant classified information with appropriate officials at the state level. We have initiated the security clearance process for state chief elections officials, using the existing clearance request process for state and local government officials.

With thousands of election jurisdictions across the country, it would be a significant challenge to provide a security clearance to every official with election responsibilities. While security clearances allow officials to better understand the classified context around cyber threat information, it is important to note that the Department is committed to declassifying as much information as possible in order to allow for the broadest dissemination and network protection. For instance, prior to the 2016 election, while information related to sources and methods remained classified, to the extent possible, the federal government declassified certain information related to attribution as well as technical cyber threat information that election officials could use to defend their networks.