Office of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

SEP 22 2017

The Honorable Richard J. Durbin
United States Senate
Washington, DC 20510

Dear Senator Durbin:

Thank you for your May 9, 2017 letter. Acting Secretary Duke asked that I respond on her behalf.

Safeguarding and securing cyberspace is a core homeland security mission. At the Department of Homeland Security (DHS), we work with Federal Government agencies; state, local, tribal, and territorial governments; the private sector; and international partners to share cyber threat information, promote the adoption of best practices; identify, detect, and mitigate malicious cyber activity; assess and mitigate vulnerabilities; and respond to cyber incidents. This collaborative approach strengthens the security and resilience of government and critical infrastructure systems essential to providing critical services.

In response to malicious cyber activity during the 2016 elections in the United States, DHS conducted unprecedented outreach and provided cybersecurity assistance to state and local election officials. In addition to the work before and after Election Day to secure our elections, DHS has also engaged with our allies abroad, including France, to assist with protecting their own elections. By establishing election infrastructure as a critical infrastructure subsector, DHS is formalizing the prioritization of assistance similar to the financial services sector or the electric power grid. Enclosed you will find responses to your questions about the French election.

Thank you again for your letter. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

Christopher C. Krebs
Senior Official Performing the Duties
of the Under Secretary

The Department of Homeland Security's Response to
Senator Durbin's May 9, 2017 Letter

1. **Does the Administration assess that Russians launched cyber attacks and other acts of disinformation on the French election?**

   I understand the Office of the Director of National Intelligence is providing a response to your letter that includes information related to the intelligence community's assessment of attribution concerning malicious cyber activity related to the French Presidential election.

2. **Has the Administration publicly or privately condemned the Russian actions against the French and other Western elections?**

   The Administration has made cybersecurity a top priority, including a range of actions currently underway in response to Executive Order 13800 entitled, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*. Regarding public or private diplomatic messages in response to malicious cyber activity, other Departments are in a better position to respond.

3. **What has the Administration done to help the French and other Western allies identify and protect against Russian cyber and disinformation campaigns? What is it doing to warn and help allies of such future actions?**

   The Department of Homeland Security's (DHS) National Cybersecurity and Communications Integration Center (NCCIC) shares information with international partners related to cyber threats. Such information enables network defenders to take action to prevent and mitigate malicious cyber activity. For instance, prior to the French and German elections, NCCIC engaged with its French and German partners to provide an overview of the actions DHS took prior to the 2016 election to mitigate potential vulnerabilities to election infrastructure. Other Departments can speak to their own efforts to assist our allies in response to these cyber threats.

4. **What is the Administration doing to retaliate against such attacks?**

   Through network protection efforts, including sharing cyber threat and vulnerability information and actionable mitigation measures with partners, DHS plays an important role in deterring adversaries in cyberspace. Other Departments are in the best position to address additional actions under their own authorities and responsibilities.

5. **What is the Administration doing to thwart such attacks against future elections in the United States and to help U.S. state governments do the same?**

   Given the vital role that elections play in a free and democratic society, earlier this year, the Secretary of Homeland Security determined that election infrastructure should be designated as a critical infrastructure subsector. With the establishment of an Election Infrastructure

epic.org EPIC-17-03-31-DHS-FOIA-20190910-CISA-Senator-Durban-Response-Letter 000002

subsector, DHS and its federal partners have been formalizing the prioritization of cybersecurity assistance and protections for owners and operators of election infrastructure similar to those provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities. Participation in the subsector is voluntary, and the establishment of a subsector does not create federal regulatory authority. Elections continue to be governed by state and local officials, but with additional prioritized efforts by the Federal Government to provide voluntary security assistance.

DHS is engaged with stakeholders across the spectrum to increase awareness of potential vulnerabilities and enhance the security of U.S. election infrastructure. DHS continues to work with a diverse set of stakeholders to plan, prepare, and mitigate risk to the election infrastructure. State and local election officials have a long-standing history of working both individually and collectively to reduce risks and ensure the integrity of their elections. In partnering with these officials through both new and existing, ongoing engagements, DHS is working to enhance efforts to secure their election systems.

Addressing cybersecurity challenges and helping our customers assess their cybersecurity risk is not new for DHS. We have three sets of cybersecurity customers: federal civilian agencies; state local, tribal, and territorial governments; and the private sector. Assistance includes three lines of business to support these customers: information sharing, best practices, and technical assistance. Support to state and local customers, such as election officials, is part of our daily operations.

DHS is working collaboratively with election officials and vendors of election infrastructure to establish coordinating councils that will be used to develop a physical security and cybersecurity strategy for the Election Infrastructure subsector and define how the Federal Government will work with election officials and vendors going forward. The coordinating councils will also be used to regularly share information on relevant threats and vulnerabilities quickly and efficiently so that owners and operators can manage their risk. Historically, DHS has not had active engagement directly with the state and local election community, so we are working on broadening and deepening those relationships, identifying requirements, and educating the community on our capabilities.

Through engagements with state and local election officials, including working through the Sector Coordinating Council, DHS actively promotes a range of services, which include:

Cyber hygiene service for Internet-facing systems: This voluntary service is conducted remotely, after which DHS can provide state and local officials with a report identifying vulnerabilities and mitigation recommendations to improve the cybersecurity of systems connected to the Internet, such as online voter registration systems, election night reporting systems, and other Internet-connected election management systems.

Risk and vulnerability assessments: These assessments are more thorough and performed 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

epic.org EPIC-17-03-31-DHS-FOIA-20190910-CISA-Senator-Durban-Response-Letter 000003

recommended mitigations following the testing. These assessments are available on a limited, first-come, first-served basis.

Incident response assistance: DHS encourages state and local election officials to report suspected malicious cyber activity to the NCCIC. On request, the NCCIC can provide on-site assistance in identifying and remediating a cyber incident. Information reported to the NCCIC is also critical to the Federal Government's ability to broadly assess malicious attempts to infiltrate election systems. This technical information will also be shared with other states to assist their ability to defend their own systems from similar malicious activity in a way that protects the identity of affected entities from disclosure.

Information sharing: DHS will continue to share relevant information on cyber incidents through multiple means, including sharing via the Multi-State-Information Sharing and Analysis Center (MS-ISAC). Election officials can connect with their state Chief Information Security Officer or the MS-ISAC directly as one way to benefit from this partnership and rapidly receive information they can use to protect their systems. State election officials may also receive incident information directly from the NCCIC.

Classified information sharing: DHS provides classified briefings to cleared stakeholders upon request, and as appropriate and necessary, including intelligence assessments from DHS's Office of Intelligence and Analysis.

Field-based cybersecurity advisors and protective security advisors: DHS has personnel available in the field who can provide actionable information and connect election officials to a range of tools and resources available to improve the cybersecurity preparedness of election systems and the physical site security of voting machine storage and polling places. These advisors are also available to assist with planning and incident management assistance for both cyber and physical incidents.

Physical and protective security tools, training, and resources: DHS provides advice and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff on identifying and reporting suspicious activities, active shooter scenarios, and what to do if they suspect an improvised explosive device.

6. **What is the Administration doing with Congressional leadership to pass appropriate legislation sanctioning Russia for its actions and preventing such attacks such attacks in the future?**

Other Departments responsible for sanctions policy and implementation are in the best position to respond to a question on such activity.

epic.org EPIC-17-03-31-DHS-FOIA-20190910-CISA-Senator-Durban-Response-Letter 000004