Secretary
U.S. Department of Homeland Security
Washington, DC 20528

Homeland Security

September 17, 2016

The Honorable Thomas R. Carper
Ranking Member
Committee on Homeland Security
and Government Affairs
United States Senate
Washington, DC 20510

Dear Ranking Member ~~Carper~~ Tom:

Thank you for your August 8, 2016 letter.

In recent months we have seen cyber intrusions involving political institutions and personal communications. We have also seen some efforts at cyber intrusions of voter registration data maintained in state election systems. We have confidence in the overall integrity of our electoral systems. It is diverse, subject to local control, and has many checks and balance built in.

Nevertheless, we must face the reality that cyber intrusions and attacks in this country are increasingly sophisticated, from a range of increasingly capable actors that include nation-states, cyber hacktivists, and criminals. In this environment, we must be vigilant.

In August, I hosted a phone call with election officials from across the country and representatives from the U.S. Election Assistance Commission, the National Institute of Standards and Technology, and the Department of Justice to discuss the cybersecurity of election infrastructure. I began by recognizing the important work state and local officials across the country have already begun to reduce risks and ensure the integrity of their elections. I also emphasized that cyber experts at the Department of Homeland Security (DHS) are available to assist state and local election officials in securing their systems, just as we do for businesses and other entities across the spectrum of the private and public sectors. This includes the most cybersecurity sophisticated businesses in corporate America.

It is important to emphasize what DHS assistance does not entail. Regardless of whether some aspect of election infrastructure is considered critical infrastructure, DHS assistance is strictly voluntary and does not entail regulation, binding directives, and is

not offered to supersede state and local control over the process. The DHS role is limited to support only.

Subject to resource constraints, the following DHS services can be made available to state and local officials almost immediately, prior to November 8:

Cyber hygiene scans on Internet-facing systems. These scans are conducted remotely, after which we 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. Once an agreement to provide these services is reached, DHS can complete this scan and provide the report within one week. This can be followed by weekly reports on an ongoing basis. Several state and local agencies are already employing DHS cyber hygiene scans on parts of their networks.

Risk and vulnerability assessments. These assessments are more thorough and done on-site by DHS cybersecurity experts. They typically require 2-3 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. Given resource and time constraints, we can only conduct these assessments on a limited, first-come, first-serve basis.

The National Cybersecurity and Communications Integration Center (NCCIC). The NCCIC is DHS's 24x7 cyber incident response center. We encourage 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.

Information sharing. DHS will continue to share relevant information on cyber incidents through multiple means. The NCCIC works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide threat and vulnerability information to state and local officials. The MS-ISAC is partially grant-funded by DHS and has a cleared representative co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers. All states are members of the MS-ISAC. DHS requests that election officials connect with their state CIO 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. Upon request, and subject to resource constraints, DHS is able to provide classified briefings to cleared state officials as appropriate and necessary.

Sharing of best practices. DHS is publishing best practices for securing voter registration databases and addressing potential threats to election systems from ransomware.

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.

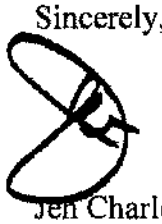
Physical and protective security tools, training, and resources. DHS provides advice and tools to improve the security of polling sites and other physical election infrastructure. This guidance can be found at www.dhs.gov/hometown-security. This guidance helps to train administrative and volunteer staff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

Finally, consistent with the Cybersecurity National Action Plan, DHS is working to raise the level of cybersecurity in our electoral infrastructure over the long term. To help develop this plan, DHS has established an experts group comprised of academics, independent cyber security researchers, and federal partners.

In recent weeks a number of states have reached out to us with questions or for assistance. We strongly encourage more state and local election officials to do so.

Thank you again for your letter and interest in this important issue. Should you wish to discuss this matter further, please do not hesitate to contact me.

Sincerely,



Jeh Charles Johnson