Written Testimony

of

Christopher Krebs
Senior Official Performing the Duties of the Under Secretary
National Protection and Programs Directorate
U.S. Department of Homeland Security

Before the
United States House of Representatives
Committee on Oversight and Government Reform
Subcommittees on Information Technology and Intergovernmental Affairs

Regarding
Cybersecurity of Voting Machines
November 29, 2017

Chairman Hurd, Chairman Palmer, Ranking Member Kelly, Ranking Member Demings and members of the Subcommittees, thank you for inviting me to participate in today's hearing on securing our elections from malicious cyber activity. This is an especially timely topic given the elections earlier this month. As you know, the Department of Homeland Security (DHS) performs a critical mission focused on reducing and eliminating threats to the nation's critical physical and cyber infrastructure, including how it relates to our elections.

Given the vital role that elections play in a free and democratic society, the Secretary of Homeland Security determined that election infrastructure should be designated as a critical infrastructure subsector. With the establishment of an Election Infrastructure Subsector (EIS), the DHS National Protection and Programs Directorate (NPPD) and federal partners have been formalizing the prioritization of ***voluntary*** cybersecurity assistance for election infrastructure similar to that which is provided to a range of other critical infrastructure entities, such as financial institutions and electric utilities.

During the 2016 election period and since that time, the federal government and election officials have been meeting regularly to share cybersecurity risk information and to determine effective means of assistance. Recently, the EIS Government Coordinating Council (GCC) met to establish goals and objectives, to develop plans for the EIS partnership, and to lay the groundwork for developing an EIS Sector Specific Plan (SSP). The GCC framework provides a well-tested mechanism across critical infrastructure sectors for sharing threat information between the federal government and council partners, advancing risk management efforts, and prioritizing services available to sector partners in a trusted environment. EIS-GCC representatives include DHS, the U.S. Election Assistance Commission (EAC), the National Institute of Standards and Technology (NIST), the Federal Buruea of Investigation (FBI), the Department of Defense (DoD), and key state and local election officials. Participation in the council is entirely voluntary and does not change the fundamental role of state and local jurisdictions in overseeing elections.

In addition to the work of the EIS-GCC, DHS continues to engage state and local elections officials – coordinating requests for assistance, risk mitigation, information sharing, and incident coordination resources and services. In order to ensure a coordinated approach across DHS, NPPD has brought together stakeholders from across the Department as part of an Election Task Force (ETF). The ETF increases the Department's efficiency and efficacy in understanding, responding to, communicating, and sharing information related to cyber threats. The ETF serves to provide actionable information to assist states in strengthening their election infrastructure against cyber threats.

Assessing the Threat

DHS continues to robustly coordinate with the EAC, the intelligence community, and law enforcement partners. Among non-federal partners, DHS has been engaging state and local officials, as well as relevant private sector entities, to assess the scale and scope of malicious cyber activity potentially targeting the U.S. election infrastructure. In addition to working directly with state and local officials, we partnered with stakeholders to analyze relevant cyber data, including the Multi-State Information Sharing and Analysis Center (MS-ISAC), the

National Association of Secretaries of State and the National Association of State Election Directors.

We also used our field personnel deployed around the country, to help further facilitate information sharing and enhance outreach. Such engagement paid off in terms of identifying suspicious and malicious cyber activity targeting the U.S. election infrastructure. A body of knowledge grew throughout the summer and fall of 2016 about suspected Russian government cyber activities, and understanding that helped drive collection, investigations, and incident response activities. On October 7, 2016, DHS and the Office of the Director of National Intelligence (ODNI) released a joint statement to the public on election security and urged state and local governments to be vigilant and seek cybersecurity assistance.

We continue to assess that mounting widespread cyber operations against U.S. voting machines at a level sufficient to affect a national election would require a multiyear effort with significant human capital and information technology (IT) resources available only to nation-states. The level of effort and scale required to significantly change a national election result, however, would make it nearly impossible to avoid detection.

Enhancing Security for Future Elections

DHS continues to focus our efforts on ensuring a coordinated response from DHS and its federal partners to plan, prepare, and mitigate risk to the election infrastructure. We recognize that working with stakeholders is the only sure way to ensure more secure elections. Based on our assessment of activity observed in the last election, DHS is engaged with stakeholders across the spectrum to increase awareness of potential vulnerabilities and enhance security of U.S. election infrastructure.

Our election process is governed and administered by state and local election officials in thousands of jurisdictions across the country. These officials manage election infrastructure and ensure its security on a day-to-day basis. State and local election officials across the country 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, NPPD is working to enhance their efforts to secure election systems.

Improving coordination with state and local partners: Increasingly, the nation's election infrastructure leverages IT for efficiency and convenience. Similar to other IT systems, reliance on digital technologies introduces new cybersecurity risks. NPPD helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage some of these cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we have been working with election officials to share information about cybersecurity risks, and to provide voluntary resources and technical assistance.

DHS works with the MS-ISAC to provide threat and vulnerability information to state and local officials. Created by DHS over a decade ago, the MS-ISAC is partially funded by NPPD. The MS-ISAC's membership is limited to state and local government entities, and all

fifty states and US territories are members. It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for state chief information officers.

Providing technical assistance and sharing information: Through engagements with state and local election officials, including working through the Sector Coordinating Council, NPPD actively promotes a range of services to include but are not limited to the following:

Cyber hygiene service for Internet-facing systems: This voluntary service is conducted remotely, afterwards, NPPD provides 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. During the 2016 election, we provided cyber hygiene services to 33 state and 36 local election jurisdictions.

Risk and vulnerability assessments: These assessments are more thorough and executed on-site by NPPD cybersecurity experts. These evaluations require two to three weeks and include a wide range of vulnerability testing services, focused on both internal and external systems. When NPPD conducts these assessments, we provide a full report of vulnerabilities and recommended mitigations following the testing. These assessments are available on a limited, first-come, first-served basis.

Incident response assistance: 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 state officials so they have the 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 MS-ISAC, and election officials can connect with the MS-ISAC or their State Chief Information Officer 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. In 2016, best practices, cyber threat information, and technical indicators, some of which had been previously classified, were shared with election officials in thousands of state and local jurisdictions.

Classified information sharing: DHS provides classified briefings to cleared stakeholders upon request, as appropriate and necessary.

Field-based cybersecurity advisors and protective security advisors: DHS has more than 130 cybersecurity and protective security personnel available to provide actionable information and connect election officials to a range of tools and resources to improve the cybersecurity preparedness of election systems and to secure the physical site security of voting

machine storage and polling places. These advisors are also available to assist with planning and incident management for both cyber and physical incidents.

Physical and protective security tools, training, and resources: NPPD 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 local NPPD PSAs for access to DHS resources.

2017 Elections and Beyond

This hearing is timely given the elections earlier this month. We have been working with election officials in all states to enhance the security of their elections by volunteering operations support and by establishing essential lines of communications with election infrastructure partners at all levels – public and private – for reporting both suspicious cyber activity and incidents. To quickly and effectively evaluate and triage any potential cyber-related events related to Election Day, DHS enhanced its state of readiness. Our goal was to enhance transparency and have visibility of aggregated elections-related cybersecurity efforts. These enhanced operations exercised interagency coordination, incident escalation, and incident communications to better improve guidance and planning in preparation for elections operations in 2018 and beyond.

In closing, the fundamental right of all citizens to be heard by having their vote accurately counted is at the core of our American values. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society. We have confidence in the overall integrity of our electoral system. Our voting infrastructure is diverse, subject to local control, and has many checks and balances. As the threat environment evolves, the Department will continue to work with state and local partners to enhance our understanding of the threat; and to provide essential physical and cybersecurity tools and resources available to the public and private sectors to increase security and resiliency.

Thank you for the opportunity to appear before the Subcommittees today. I look forward to your questions.