TESTIMONY

OF

DR. ANDY OZMENT
ASSISTANT SECRETARY
OFFICE OF CYBERSECURITY AND COMMUNICATIONS
NATIONAL PROTECTION AND PROGRAMS DIRECTORATE
U.S. DEPARTMENT OF HOMELAND SECURITY

BEFORE
THE

HOUSE COMMITTEE ON OVERSIGHT AND GOVENRMENT REFORM
SUCOMMITTEE ON INFORMATION TECHNOLOGY
U.S. HOUSE OF REPRESENTATIVES
WASHINGTON, D.C.

CYBERSECURITY: ENSURING THE INTEGRITY OF THE BALLOT BOX

SEPTEMBER 28, 2016

Chairman Hurd, Ranking Member Kelly, members of this Committee, thank you for the opportunity to testify. Citizens in several states and the District of Columbia have already begun voting in the 2016 general election. A majority of states and the District of Columbia allow early voting prior to November. By November 8, eligible residents of every state and territory, from every precinct, will be able to cast their votes for President, members of Congress, their local leaders, and ballot initiatives. At the core of our American values is the fundamental right of all citizens to make their voices heard by having their vote counted. Ensuring the integrity of our electoral process is a vital national interest and one of our highest priorities as citizens in a democratic society.

Our election system is funded and governed by state and local governments in thousands of jurisdictions across the country and administered by the dedicated local officials residing in those places. It is local citizens—often dedicated volunteers—who staff polling locations in their precincts and transmit the results to their election officials. Importantly, state and local officials across the country have already been working individually and collectively to reduce risks and ensure the integrity of their elections. Through existing and ongoing engagements we look forward to partnering with them to continue the work they have already started.

Increasingly, the nation's election infrastructure leverages information technology for efficiency and convenience. And like other systems, reliance on digital technologies introduces new cybersecurity risks. However, the diverse and dispersed nature of our election infrastructure provides inherent resilience and presents real challenges to a coordinated, significant incident having an impact on election results. Our National Cybersecurity and Communications Integration Center (NCCIC) helps stakeholders in federal departments and agencies, state and local governments, and the private sector to manage their cybersecurity risks. Consistent with our long-standing partnerships with state and local governments, we are working with election officials to share information about cybersecurity risks and to provide voluntary resources from the Department upon request.

Recent news reports have mentioned cyber incidents in several states this year related to election infrastructure, specifically voter registration databases. Our NCCIC has shared actionable information through direct outreach to state and local governments and through the Multi-State Information Sharing and Analysis Center (MS-ISAC), to enhance situational awareness and provide election officials with the information needed to protect themselves from similar incidents. Importantly, none of the reported incidents contain indications of malicious activity that would impact the ability of voters to cast their ballots.

Addressing cybersecurity challenges such as these is not new for our Department. At the NCCIC, we have three sets of cybersecurity customers: federal civilian agencies; state local, tribal, and territorial governments; and the private sector. The NCCIC has three lines of business to support these customers: information sharing, bet practices, and incident response. Support to state and local customers, such as election officials, is part of the NCCIC's daily operations.

In August 2016, Secretary Johnson hosted a phone call with election officials from across the country that included 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. The Secretary offered assistance from the NCCIC to assist state and local election officials in securing their systems. The NCCIC provides this same assistance on an ongoing basis to public and private sector partners upon request. Such assistance is voluntary and does not entail regulation, binding directives, or any kind of federal "takeover," as has been suggested by some in public discussion. No state or local election official should hesitate to request our assistance based on that misperception. DHS is only providing assistance in support of state and local authorities when they request it.

Through engagements with state and local officials, we are actively promoting a range of available services to include:

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.

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. Given resource and time constraints, we can only conduct these assessments 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 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 was created by DHS over a decade ago and is grant funded by DHS. The MS-ISAC role is restricted to state and local government entities. It has representatives 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. Election officials can connect with their state CIO 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. 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.

Finally, 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 cybersecurity researchers, and federal partners.

Before closing, I want to reiterate that we have confidence in the overall integrity of our electoral system. Our voting infrastructure is is diverse, subject to local control, and has many checks and balances built in. As the threat environment evolves, the Department will continue to work with state and local partners to make essential physical and cybersecurity tools and resources available to the public and private sectors.

Thank you for the opportunity to testify, and I look forward to any questions.