Options to protect and defend US election infrastructure and US political parties

Election infrastructure includes a diverse set of assets, systems, and networks critical to the administration of the election process. Based on Department of Homeland Security (DHS) analysis of the election process, the following represents key parts of the assets, systems, and networks most critical to the security and resilience of the election process, both physical locations and information and communication technology. For this effort, the term "election infrastructure" refers to the information, capabilities, physical assets and technologies which enable the registration and validation of voters; the casting, transmission, tabulation, and reporting of votes; and the certification, auditing, and verification of elections. Election infrastructure is inclusive of but not limited to the following components.

- Physical locations:
    - Storage facilities, which may be located on public or private property that may be used to store election and voting system infrastructure before Election Day.
    - Polling places (including early voting locations), which may be physically located on public or private property, and may face physical and cyber threats to their normal operations on Election Day.
    - Centralized vote tabulation locations, which are used by some States and localities to process absentee and Election Day voting materials.
- Information and communication technology (ICT):
    - Information technology infrastructure and systems used to maintain voter registration databases.
    - Voting systems and associated infrastructure, which are generally held in storage but are located at polling places during early voting and on Election Day.
    - Information technology infrastructure and systems used to manage elections, which may include systems that count, audit, and display election results on election night on behalf of State governments, as well as for postelection reporting used to certify and validate results.

The options and recommendations below focus on the cybersecurity of the ICT portion of election infrastructure.

Protecting and defending this infrastructure is the responsibility of state and local governments and election officials. DHS assists State, Local, Tribal, and Territorial (SLTT) governments, on a voluntary basis, with the management of their cyber risk.

This includes tools, services, and capabilities that can help election officials protect and defend this infrastructure.

DHS's voluntary approach preserves the ability of the system owner to make appropriate risk decisions for their own networks. States have sovereign control over the conduct and administration of elections, and the Federal government's work to assist election officials in their security efforts does not attempt to alter this sovereignty.

DHS encourages election officials to take measures to protect their systems from cyber incidents and does not seek to compel or force security compliance. This remains true even if election infrastructure is designated as critical infrastructure, a topic that will be discussed in more detail below.

In addition to election officials, private sector election infrastructure vendors are instrumental to the security of information and communication technology used in elections. These private sector entities design, manufacture, sell, and maintain, in coordination with election officials, systems and assets that are part of election infrastructure. Many of these systems and assets are due to be replaced or upgraded and it is imperative that the Federal government work with these private sector vendors to ensure that their products are designed to be secure from cyber incidents.

US political parties, which are non-governmental organizations, also are vital to the conduct of our elections. The tools and services that the Federal government can provide to them to protect the information technology and communications systems and networks which parties employ in their professional capacity are similar, but not identical, to what can be provided to election officials and vendors. For example, DHS furnishes some capabilities for SLTT governments, like those at the Multi-State Information Sharing and Analysis Center (MS-ISAC), which are not available to nongovernment stakeholders. DHS does provide a wide range of resources to empower non-governmental organizations to enhance the resilience of their physical and cyber infrastructure. Political entities are eligible for many of these resources, by request.

It is important to note the importance of the media in the election process. Information technology products and services are used by the media to report unofficial, preliminary election results received from election night reporting systems hosted by election officials. These unofficial results are analyzed with polling data to provide the public with information on election night. The media plays a critical role in ensuring the public's confidence in the election results, and any cyber incident that targets the media's ability to report accurate information may have an effect on the public's confidence in our electoral process. Recognizing the vital position of the media in this and other aspects of life, media organizations have been important participants of the Entertainment and Media subsector of the Commercial Facilities critical infrastructure sector. While the services and capabilities below have been organized in a manner that focuses on their relevance to election audiences, the Federal government also works with the media in a similar manner to ensure its security and resilience as a part of our Nation's critical infrastructure through the National Infrastructure Protection Plan.

Unless indicated otherwise, the following services and capabilities are available to SLTT election infrastructure owners, private sector vendors of election infrastructure, as well as US political parties. Much of the work below can and will be done by DHS under its mandate to assist SLTT governments and the private sector in the management of their cyber risk. The vast majority of what is recommended is funded by the US Government. Election officials operate under constrained budgets and often require additional funds to implement best practices and recommended risk management improvements. Opportunities to alleviate the financial burden placed on SLTT for acquiring election-security capabilities would likely be well received and improve the cybersecurity of their election infrastructure. Recommendations are provided in areas where additional authorities or resources are required.

Designation of Election Infrastructure as Critical Infrastructure

The nation's critical infrastructure provides the essential services and backbone for the economy, security and health. Currently, DHS designates 16 critical infrastructure sectors. Designation of a sector as critical infrastructure helps the Federal government prioritize and align support and resources.

An explicit designation of election infrastructure as critical infrastructure would enable the use of existing policy mechanisms designed to protect critical infrastructure from cyber attacks. This designation would likely include the establishment of an Election Infrastructure sector or sub-sector of critical infrastructure. Designation as critical infrastructure would not alter the Federal government's role in elections and would not provide any regulatory authority or oversight over state control of the election process. Designation would provide the following benefits:

- Owners and operators of election infrastructure would be covered explicitly by the international peacetime cyber norms, including the prohibition on peacetime cyber attacks against critical infrastructure.
- Under Executive Order 13694, the Secretary of Treasury can designate persons responsible for cyber enabled activities that harm or compromise a computer that supports an entity in a critical infrastructure sector, which would now explicitly include election infrastructure.
- Election Infrastructure would become a priority under the National Infrastructure Protection Plan. This would allow DHS to prioritize resources and continue the

election security work across administrations at a critical time given that 43 states are set to modernize their election infrastructure in the next 4 years.

- Critical infrastructure information about systems and assets voluntarily submitted to DHS for validation as Protected Critical Infrastructure Information (PCII) is exempt from the Freedom of Information Act (FOIA), use in civil litigation, and regulatory use. A designation would reinforce that information pertaining to election infrastructure would qualify for these protections. This will encourage greater sharing of information and collaboration.
- The Federal Government would be allowed to convene meetings with state and local election officials, federal officials, and election infrastructure vendors under the Critical Infrastructure Protection Advisory Council (CIPAC) framework. This would allow for participants to have open and frank discussions regarding sensitive vulnerability information. These meetings could be closed to the public and exempt from the Federal Advisory Committees Act (FACA) to restrict broad dissemination of this sensitive vulnerability information.

Recommendations:

- Proceed with the designation of election infrastructure as critical infrastructure to enable the above benefits and protections.
- Charter the existing Election Infrastructure Cybersecurity Working Group under CIPAC and incorporate election infrastructure vendors into the group to share cybersecurity information that will improve supply chain management, security development, patch management, and other aspects of the product development cycle.

Encourage Information Sharing and use of Coordination Centers

DHS's National Cybersecurity and Communications Integration Center (NCCIC) is authorized by statute in section 227 of the Homeland Security Act with a wide range of cybersecurity information sharing and coordination authorities. 6 U.S.C. § 148(c). Executive Order 13636 directs the United States Government to increase the volume, timeliness, and quality of cyber threat information shared with owners and operators of information systems so that these entities may better protect and defend themselves against cyber threats. DHS executes several programs and capabilities to connect owners and operators of cyber risk information rapidly. These programs are currently available to election officials, election infrastructure vendors, and US political parties for use in protecting their systems.

- Automated Indicator Sharing (AIS): DHS's AIS program enables the exchange of cyber threat indicators between the Federal Government and non-Federal entities at machine speed. Threat indicators generally include information such as malicious IP addresses or the sender address of a phishing email, although they can also be much more complex.
- Cyber Information Sharing and Collaboration Program (CISCP): DHS's NCCIC provides a series of information sharing products that apply context and analysis to cyber threat indicators to enable effective network defense.
- Information Sharing and Analysis Organizations (ISAOs) and Information Sharing and Analysis Centers (ISACs): ISAOs and ISACs allow for sharing of security information based on affinity among members. These provide a more formalized structure for information sharing among members and between members and the Federal government. Some ISAOs and ISACs, including the Multi-State ISAC, which provides SLTT governments with a 24x7 cybersecurity operations center, also allow for the provision of technical assistance.

Recommendations:

- Publicly encourage election officials, election infrastructure vendors, and US political parties to leverage the AIS and CISCP programs to improve the security of their systems through robust information sharing and to share indicators with the Federal government.
- DHS should provide technical assistance, resources, and funding for AIS equipment to election officials, as needed. Funding sources for AIS equipment are not currently budgeted and would require additional funds.
- Publicly encourage election officials to participate in the Multi-State ISAC either through their existing state MS-ISAC member or independently.
- Publicly encourage election infrastructure vendors to join an existing ISAO or ISAC, such as the Information Technology ISAC (IT-ISAC), or establish a new ISAO for the purposes of securing election infrastructure.
- Publicly encourage US political parties to form an ISAO and recommend that the Federal government provide funding to an independent organization, such as the Election Assistance Commission, to establish this ISAO.

The federal government facilitates or provides funding for coordination centers to disseminate essential cybersecurity information among appropriate audiences and provide additional services. Where applicable, election officials, election infrastructure vendors, and US political parties would benefit from the capabilities and services provided by these centers.

- National Cybersecurity and Communications Integration Center (NCCIC): DHS's NCCIC is a 24x7 cyber situational awareness, incident response, and management center that integrates cyber and communications for the Federal Government, intelligence community, and law enforcement. *See* 6 U.S.C. § 148. The NCCIC is the primary platform to coordinate the Federal Government's asset response to cyber incidents, as outlined in Presidential Policy Directive 41 (PPD-41) on "United States Cyber Incident Coordination," and is authorized by statute with both coordination authorities as well as actual incident response authorities. 6 U.S.C. § 148(c).
- National Cyber Investigative Joint Task Force (NCIJTF): The NCIJTF is a multi-agency center hosted by the Federal Bureau of Investigation and is the primary platform to coordinate the Federal Government's threat response, as outlined in PPD-41. The NCIJTF is chartered under paragraph 31 of National Security Presidential Directive-54/Homeland Security Presidential Directive-23.
- Multi-State Information Sharing and Analysis Center (MS-ISAC): DHS also funds the MS-ISAC. MS-ISAC was established to provide cybersecurity capabilities and situational awareness information tailored to the networks and essential functions of state governments, which can include election infrastructure. The MS-ISAC coordinates closely with the NCCIC, ensuring effective lines of communication between the two Centers. (*Available to state and local governments only*)

Recommendation:

- Publicly encourage election officials, election infrastructure vendors, and US political parties to engage regularly with the above cyber centers and leverage the information resources provided by them to improve their cyber security and report cyber incidents to these centers, when appropriate.

Encourage Adoption of Cybersecurity Best Practices and Standards

- The majority of threat actors can be stopped by adopting best practices and establishing and implementing cybersecurity standards. The Federal government works to develop and promote cybersecurity best practices and standards to our stakeholders, and these can be leveraged by election officials, election infrastructure vendors, and US political parties. Consistent with, among other authorities, the NCCIC's statutory mandate to "provid[e] "information and recommendations on security and resilience measures to Federal and non-Federal entities," it develops and disseminates best practices documents that strengthen recipients' understanding of appropriate security measures. *See* 6 U.S.C. § 148(c)(7). These products are available to all interested parties but may be tailored to a specific issue or sector. In the 2016 election cycle, DHS developed and distributed a best practice document on protecting voter information within online voter registration databases.

- Per Executive Order 13636, the US Government has worked with the private sector to develop the NIST Cybersecurity Framework as the common guidance document for cybersecurity best practices. DHS works to increase adoption of the NIST Cybersecurity Framework by developing guidance, establishing trusted relationships with partners, and educating implementers such as chief information and information security officers.
- The National Institute of Standards and Technology (NIST) and the US Election Assistance Commission (EAC) co-lead a committee that develops the Voluntary Voting System Guidelines, which include security measures for voting systems. Additionally, EAC has a certification process to test and certify voting systems according to these guidelines. DHS cybersecurity professionals are providing input on the voluntary standards being established.

Recommendations:

- Publicly encourage election officials, election infrastructure vendors, and US political parties to adopt the Cybersecurity Framework and provide them with the necessary resources to do so through DHS's Critical Infrastructure Cybersecurity Voluntary Program.
- DHS should work with Federal partners and election infrastructure stakeholders to continue the development of best practices documents focused on the cybersecurity of election infrastructure.
- DHS should continue to work with NIST and the EAC to provide inputs related to current cybersecurity issues and threats for the Voluntary Voting Systems Guidelines and the EAC's Board of Advisors and Standards Board.

Encourage Use of Cyber Risk Assessment and Management Capabilities

DHS provides cyber risk assessment capabilities to help election officials, election infrastructure vendors, and US political parties to manage their cyber risk. This falls under NCCIC's statutory mandate to provide, upon request, "timely 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." 6 U.S.C. § 148(c)(6); *see also* 6 U.S.C. § 121(d)(2). These risk assessments help organizations improve their own security and establish a productive relationship with the Federal government. The following programs are free to stakeholders, which is especially important for election officials who operate with constrained budgets.

- Field-based Cyber Security Advisors and Protective Security Advisors provide actionable information and connect election officials, election infrastructure vendors, and US political parties to a range of tools and resources available to improve the cybersecurity preparedness of election infrastructure from physical and cyber threats. These advisors are also available to assist with planning and incident management assistance for both cyber and physical incidents.
- Cyber Resilience Reviews are no-cost, voluntary, non-technical assessments to evaluate operational resilience and cybersecurity capabilities within organizations. These reviews seek to understand an organization's capacities and capabilities in performing, planning, managing, measuring, and defining cybersecurity practices and behaviors.
- Cyber Hygiene scans are voluntary assessments of internet-accessible systems for known vulnerabilities and configuration errors. DHS provides a weekly report to participants of this service that includes remediation and mitigation recommendations to address identified vulnerabilities that can be used to improve their cybersecurity posture. In the lead up to the 2016 election, 33 states and 36 counties employed DHS Cyber Hygiene scans on parts of their internet-facing election infrastructure. DHS continues to provide this voluntary assessment service to election officials.
- Risk and Vulnerability Assessments (RVAs) include a wide range of penetration testing services and web application and database testing. RVAs are in-depth assessments conducted by teams of expert DHS personnel to determine whether malicious actors can defeat security controls employed on a given network or system.

Recommendations:

- Publicly encourage election officials, election infrastructure vendors, and US political parties to take advantage of these DHS programs.
- In addition to the free services discussed above, propose DHS-issued grant funding for state and local election officials to acquire or develop capabilities and services that will improve the cybersecurity of their election infrastructure. Election officials operate under constrained budgets and often require additional funds to implement best practices and risk management improvements that are identified via the above programs. (*Limited to state and local election officials*)

Provide and Enable Incident Response Capabilities

The Federal Government provides robust incident response capabilities and coordination mechanisms to respond to and recover from cyber incidents affecting election infrastructure. PPD-41 sets forth principles governing the Federal government's response to cyber incidents, and for significant cyber incidents, as defined in the PPD, it establishes lead Federal agencies and an architecture for coordinating the broader Federal response. The National Cyber Incident Response Plan (NCIRP), called for in PPD-41, provides the strategic framework for how the Federal government works with stakeholders in the private sector and SLTT governments during a cyber incident. Federal agencies work together to help affected entities understand the incident, link related incidents, and share information to rapidly resolve the situation in a manner that protects privacy and civil liberties. Incident response capabilities are available through DHS and the FBI; the cyber centers they respectively lead, the NCCIC and NCIJTF; and additionally for SLTT election officials, the MS-ISAC.

Recommendations:

- Ensure that election officials, election infrastructure vendors, and US political parties are aware of the incident response capabilities provided by DHS, FBI, and other Federal agencies.
- Encourage election officials, election infrastructure vendors, and US political parties to share information on cyber incidents that affect them with the Federal government and, when necessary, request technical assistance to respond to and recover from the cyber incident.
- DHS, in coordination with other Federal government partners, should work with election officials, election infrastructure vendors, and US political parties to build an Election Infrastructure Cyber Response Plan that details how election infrastructure owners and operators leverage the NCIRP and respond to a cyber incident.
- DHS, in coordination with other Federal government partners, should regularly conduct exercises with election officials, election infrastructure vendors, and US political parties to test the Election Infrastructure Cyber Response Plan, build capacity with partners, and improve incident response and coordination capabilities.