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

Homeland Security

June 13, 2017

The Honorable Claire McCaskill
Committee on Homeland Security
and Governmental Affairs
United States Senate
Washington, DC 20510

Dear Ranking Member McCaskill:

Thank you for your March 7, 2017 letter.

Critical infrastructure faces an ever-evolving range of threats, from terrorism to malicious cyber activity to natural disasters. Reducing the risks from these threats, and making our physical and cyber infrastructure more resilient and secure is an important mission of the Department of Homeland Security.

The establishment of election infrastructure as a critical infrastructure subsector within the Government Facilities Sector enables state, local, tribal, and territorial governments, and private sector owners and operators to receive prioritized assistance from the Federal Government for their efforts to mitigate risks to election infrastructure. Participation with the Federal Government, as part of this subsector, is voluntary. Responses to the questions outlined in your correspondence are enclosed.

I thank you for your continued commitment and partnership with the Department on this and many other important issues. Should you wish to discuss this further, please do not hesitate to contact me.

Sincerely,

John F. Kelly

Enclosures

cc: The Honorable Ron Johnson
Chairman

The Department of Homeland Security's Response to Senator McCaskill's March 7, 2017 Letter

The following information addresses your questions related to the Department of Homeland Security's (DHS) consideration of election infrastructure as critical infrastructure.

1. **Before the election on November 8, 2016, how many SLTT governments requested assistance?**

   For the purposes of this letter, the numbers below represent the cybersecurity services and assistance provided to state and local officials for their election infrastructure. These figures do not include the number of engagements in which DHS provides cybersecurity services and assistance to other facets of state and local governments outside of election infrastructure.

   Prior to the election, DHS offered voluntary, no-cost cybersecurity services and assistance to election officials across all 50 states. By Election Day, 33 state election offices and 36 local election offices requested and received these cyber hygiene assessments of their internet-facing election infrastructure. These cyber hygiene assessments are a no-cost, voluntary, technical assessment encompassing configuration error and vulnerability scanning. Based on findings, DHS offers recommendations on remediating the vulnerabilities. These assessments are conducted remotely and on a recurring weekly basis. In some cases, state and local election officials indicated that they were already receiving similar services, so they did not request assistance from DHS.

   In addition, one state election office requested and received a more in-depth risk and vulnerability assessment of their election infrastructure. This suite of services – also no-cost and voluntary – includes penetration testing, social engineering, wireless access discovery and identification, as well as database and operating system scanning. Several more stakeholders have signed up for this service since Election Day. These assessments do not include cyber assessments of voting machines.

   In addition to these services, DHS shared technical information with election officials to help them identify, detect, and disrupt malicious cyber activities. This included cyber threat indicators and analytic reports, including DHS/FBI Joint Analysis Reports on malicious activity by Russian civilian and military intelligence services. DHS also shared relevant best practices, such as a security tip on Securing Voter Registration Data, an interagency guidance document on ransomware, and best practices for continuity of operations related to destructive malware. These products were distributed to thousands of state and local election officials via partnerships we established with the Election Assistance Commission, the National Association of Secretaries of State, the National Association of State Election Directors, and the National Association of Counties.

   Additionally, DHS works closely with the Multi-State Information Sharing and Analysis Center (MS-ISAC), which has representatives located inside DHS's National Cybersecurity and Communications Integration Center. Funded by DHS, MS-ISAC is a key mechanism for collaborating with state and local governments to enhance their cybersecurity capabilities. Prior to the election, we coordinated with MS-ISAC on information sharing and technical assistance to state and local election officials. All state and local election officials are or could be receiving direct or indirect cybersecurity assistance from MS-ISAC, if requested.

2. **Have any new SLTT governments requested DHS assistance after the January designation?**

   Following the establishment of election infrastructure as critical infrastructure, several state and local governments requested new or expanded cybersecurity services from DHS. Specifically, an additional two states and six local governments requested to begin cyber hygiene scanning (one state has, however, ended its service agreement). DHS also received one request for the risk and vulnerability assessment service.

3. **Why does the designation include both physical and virtual assets if the 2016 election interference solely involved cyber-attacks and DHS is only offering cyber-related assistance?**

   DHS assistance to election infrastructure is focused on more than cyber threats in order to address all-hazards risk holistically. This assistance includes threat intelligence, risk assessments, training, and best practices related to physical threats. Our Nation's critical infrastructure faces an ever-evolving range of threats, from terrorist to malicious cyber activity to natural disasters. Reducing the risks from these diverse threats, and making our physical and cyber infrastructure more resilient and secure is DHS's mission. The breadth of this designation correlates to the scope of threat information and assistance that DHS can provide. For example, decision makers across the election infrastructure sub-sector may benefit from DHS-provided assistance related to physical threats targeting election infrastructure, as much as they would appreciate assistance related to cyber threats targeting election infrastructure.

   Election infrastructure includes a diverse set of assets, systems, and networks critical to the administration of the election process. When we use the term "election infrastructure," we mean the 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. Specifically, we mean at least 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.

4. **The DHS Fact Sheet on the designation explains, "Protecting and defending this infrastructure is the responsibility of state and local governments and election officials." Are states and localities or is the federal government responsible for expenses associated with the assistance and support provided by DHS?**

   Subject to the availability of its resources and at no cost to state and local governments, DHS can furnish voluntary assessments, services, and technical assistance to assist election officials in informing their decision making and election administration processes, if requested by those officials. DHS covers the expenses associated with providing these services and assistance. DHS receives annual appropriations from Congress to provide this assistance.

   State and local governments, as owners and operators of election infrastructure, are responsible for risk management, procurement, and all other decisions that are made in the administration of the elections process. DHS's establishment of a critical infrastructure sub-sector for election infrastructure has no impact on state and local control over those responsibilities.

5. **If DHS identifies vulnerabilities within an SLTT government's system that require attention, is the SLTT government responsible for the costs of implementing the solution?**

   If, in the course of providing technical services to state and local governments, DHS identifies vulnerabilities or configuration errors, DHS will offer recommendations on remediating the issues. However, the decisions of what risks and vulnerabilities are deemed acceptable is entirely the responsibility of the state or local government, as are the costs to remediate the vulnerabilities and configuration errors they deem to be unacceptable.

   In the event DHS assistance is requested, for example to respond to and recover from an incident, technical assistance services would be provided by DHS to state and local governments at no cost.

6. **If fixes are identified to improve an SLTT government's system, but that government chooses not to make the recommended adjustments to address the problem, is the state or locality liable under law?**

   DHS defers to state, local, tribal, and territorial (SLTT) government entities to analyze their potential liability under applicable law. SLTT government entities can, however, invoke the protections under the Critical Infrastructure Information Act of 2002, 6 U.S.C. § 133, when sharing information about their systems with DHS. Those protections include a protection from use of Protected Critical Infrastructure Information (PCII) in civil litigation. *See* 6 U.S.C. § 133(a)(1)(C). In DHS's view, such protection would extend to recommendations DHS provides that pertain to PCII submitted by SLTT government systems.

7. **Will the designation of election infrastructure as a critical infrastructure subsector continue under the Trump Administration?**

   There are no plans to make any changes to the designation of election infrastructure as a critical infrastructure subsector. Establishing election infrastructure as a critical infrastructure subsector within the government facilities sector enables SLTT governments, and private sector owners and operators to receive prioritized assistance from the Federal Government in their efforts to manage risks to election infrastructure. Participation with the Federal Government, as part of this subsector, is voluntary. Establishing this subsector does not involve federal intrusion, takeover, or regulation of any kind. This designation does not allow for technical access by the Federal Government into the systems and assets of election infrastructure, without voluntary legal agreements made with the owners and operators of these systems.

   This dynamic is consistent with engagements between the Federal Government and other previously established critical infrastructure sectors and subsectors, including the chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, financial services, food and agriculture, government facilities, healthcare and public health, information technology, nuclear reactors, material, waste, transportation systems, and water and wastewater systems sectors.

8. **What assistance and tools can DHS provide to SLTT governments that participate in the program?**

   Establishment of election infrastructure as a critical infrastructure enables DHS to prioritize its assistance to election officials. This includes mechanisms to rapidly share information across the community to assist with identification and mitigation of system vulnerabilities. For instance, over the previous election cycle, DHS provided voluntary, automated, un-credentialed, remote vulnerability scanning. DHS also shared cyber threat indicators, generalized vulnerability mitigation guidance, and best practices with election officials.

   Going forward, the establishment of this subsector should allow for more tailored and useful information sharing, in response to continued feedback, and iterative refinement of what information election officials would find useful. Status as a critical infrastructure subsector facilitates the following:

   1. Support for the establishment of a sector coordinating council focused on the security and resilience of election infrastructure. Coordinating councils are used to share information on vulnerabilities and threats, and to enable collaboration across federal, state, and local governments, as well as with private sector partners, to determine ways to mitigate risks. Participation is voluntary.

   2. The ability to leverage the Critical Infrastructure Partnership Advisory Council framework, where DHS can convene meetings with state and local election officials and private sector vendors. These meetings are closed to the public and exempt from Federal

Advisory Committee Act requirements to allow frank discussion about sensitive security issues.

3. The voluntary sharing of critical infrastructure information with DHS under the Critical Infrastructure Information Act of 2002, which protects information from disclosure in response to Freedom of Information Act requests, use in civil litigation, and regulatory use.

In addition to direct assistance from DHS, DHS funds the Multi-State Information Sharing and Analysis Center (MS-ISAC). State and local governments already have access to the cyber incident response capabilities of MS-ISAC; however, as a critical infrastructure subsector, election officials' incident response needs and requests for services can be prioritized, both by DHS and MS-ISAC.

9. Do you anticipate that DHS will require any additional personnel, resources, or authorities to fulfill its responsibilities associated with the designation?

DHS has been utilizing existing personnel, resources, and authorities to provide election infrastructure owners and operators with assistance. Establishing election infrastructure as a subsector of the government facilities critical infrastructure sector allows DHS to prioritize assistance using limited existing personnel, resources, and authorities.

10. How did DHS make the following determination mentioned in the ODNI report, "DHS assesses that the types of systems we observed Russian actors targeting or compromising are not involved in vote tallying?"

DHS, in coordination with partners from the Intelligence Community, federal law enforcement, and MS-ISAC, observed Russian cyber actors attempting to access voter registration databases prior to the 2016 elections. Voter registration databases are used by states to register new voters and maintain their voter rolls. Voter registration databases – distinct from voting systems – are not involved in vote tallying.

There are no indications nor observed evidence of Russian actors using cyber or physical means to target voting systems, which include voting machines (the electronic machines used by voters to cast ballots) and vote tallying systems (the electronic machines used by election officials to count and tally marked ballots). These voting systems should not have active connections to the internet during the voting process, and are rarely, if ever connected to the internet at all. Thus, they are more difficult for an adversary to access and affect remotely; however, the possibility exists that an adversary could target voting systems through close-access operations or a compromise of the supply chain.

Based on the observed threat, DHS focused its efforts on providing election officials with information to protect their internet-connected election infrastructure, such as voter registration databases, election websites that provided information for voters on where to find their polling places, and election night reporting systems.

11. **Please provide copies of any guidance or any other information provided by DHS to SLTT governments responding to the Department's designation.**

Prior to the establishment of election infrastructure as a subsector of the government facilities critical infrastructure sector, DHS and other partners shared extensive information with SLTT governments on risks and available assistance. Upon establishing election infrastructure as a subsector of the government facilities critical infrastructure sector, DHS made a Statement from the Secretary of Homeland Security and a Fact Sheet available to state and local election officials. In the following weeks, DHS provided the attached letter to the Honorable Denise Merrill, Secretary of State of Connecticut and President of the National Association of Secretaries of State, and distributed it to other Secretaries of State through the National Association of Secretaries of State. Additionally, DHS officials have participated in several speaking engagements, leveraging the attached slide deck.

Included DHS information to SLTT governments responding to the establishment of a critical infrastructure subsector:

- Statement from the Secretary on Election Infrastructure - January 6, 2017
- Election Infrastructure Fact Sheet - January 2017
- Response to Secretary of State Merrill of Connecticut - March 6, 2017
- Elections DHS SLTT Resource Brief – February 2, 2017

Homeland Security

DHS Cybersecurity: Services for State and Local Officials

February 2017

Department of Homeland Security

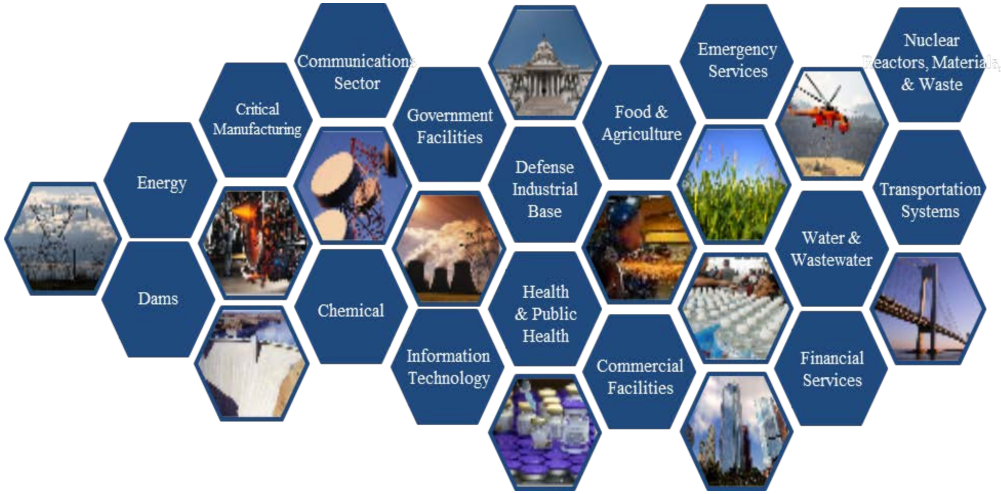
- Established in March of 2003 and combined 22 different Federal departments and agencies into a unified, integrated Department

- Homeland security is a widely distributed and diverse national enterprise
  - Collective efforts and shared responsibilities of Federal, State, local, tribal, territorial, nongovernmental, and private-sector partners to maintain critical homeland security capabilities

- 2014 QHSR Homeland Security Missions
  1. Prevent Terrorism and Enhance Security
  2. Secure and Manage Our Borders
  3. Enforce and Administer Our Immigration Laws
  4. **Safeguard and Secure Cyberspace**
  5. Strengthen National Preparedness and Resilience

National Protection and Programs Directorate

- Our mission is to protect cyber and critical infrastructure
  - Terrorism and other physical threats
  - Growing cyber threats
- Our work provides a holistic risk management approach for the 16 critical infrastructure sectors with unique legal authorities supporting true private public collaboration
- We build cyber and physical risk management capacity of Federal partners, private sector owners and operators, state and local agencies, and others



Our Cybersecurity Responsibilities

- Protect Federal Civilian Executive Branch networks from malicious cyber actors

- Support private sector and state, local, tribal, and territorial governments in the management of their cyber risk

- Provide technical assistance in the event of a cyber incident, as requested

Lines of Effort

Information Sharing

Risk Assessments

Incident Response

Cyber Ecosystem

Federal Common Cybersecurity Baseline

Interest in Elections

- As the capabilities that enable elections are becoming increasingly dependent on information and communications technology, election officials are assuming greater responsibility for the cybersecurity of these systems

- DHS has built trusted relationships with State and local IT officials to strengthen the security of their networks and is providing outreach to election officials to ensure that they are aware of the no-cost cybersecurity services that are available to them

- DHS services are available only upon request, and are voluntary; they do not entail regulation or binding directives of any kind

Cyber Hygiene (CH)

- Overview
  - Assess stakeholders internet accessible systems for known vulnerabilities and configuration errors on a recurring basis
  - DHS will work with impacted agencies to proactively mitigate threats and risks to their systems prior to exploitation by malicious third parties
  - Agency specific data is for that agency's eyes only

- Objectives
  - Establish enterprise view of the Federal, SLTT, and critical infrastructure public cybersecurity posture
  - Understand how your networks appear to an attacker

- Benefits
  - Complements an agency's existing security program and capabilities
  - Provides an objective view of an agency's public security posture
  - Reduced exposure to known threats

Risk and Vulnerability Assessment (RVA)

Service	Description
Vulnerability Scanning and Testing	Conduct Vulnerability Assessments
Penetration Testing	Exploit weakness or test responses in systems, applications, network and security controls
Social Engineering	Crafted e-mail at targeted audience to test Security Awareness / Used as an attack vector to internal network
Wireless Discovery & Identification	Identify wireless signals (to include identification of rogue wireless devices) and exploit access points
Web Application Scanning and Testing	Identify web application vulnerabilities
Database Scanning	Security Scan of database settings and controls
OS Scanning	Security Scan of Operating Systems deployed throughout network

In-depth, onsite assessments of internal and external networks

National Cybersecurity and Communications Integration Center (NCCIC)

NCCIC Classification Level:
UNCLASSIFIED
U.S. DEPARTMENT OF HOMELAND SECURITY
NCCIC

National Cybersecurity and Communications Integration Center (NCCIC)

- The DHS National Cybersecurity and Communications Integration Center (NCCIC) is a 24X7 cyber situational awareness, incident response, and management center and a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement

- The NCCIC leads the protection of the federal civilian agencies in cyberspace, provides support and expertise to critical infrastructure owners and operators, and works with the Multi-State Information Sharing and Analysis Center (MS-ISAC) to provide information to SLTT governments

National Cybersecurity and Communications Integration Center (NCCIC)

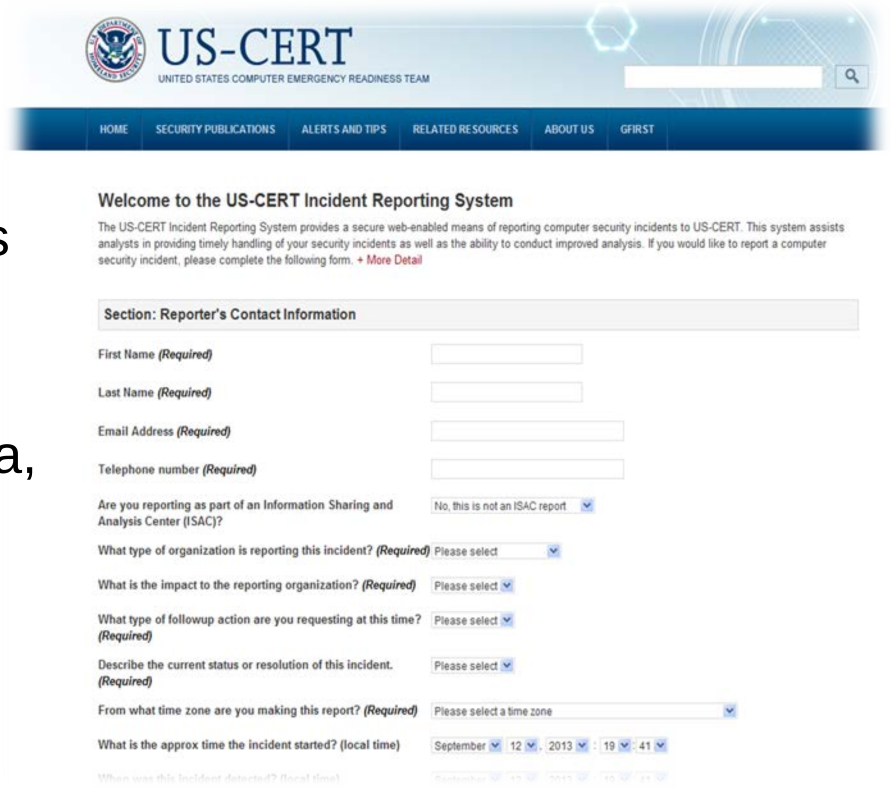
Reporting an Incident

The NCCIC operates 24x7x365 and can be reached at 1-888-282-0870 or by visiting https://forms.us-cert.gov/report.

When to Report an Incident

If there is a confirmed cyber or communications event or incident that:

- Affects core government functions
- Affects critical infrastructure functions
- Results in a significant loss of data, system availability or control of systems
- Indicates malicious software is present on critical systems



Welcome to the US-CERT Incident Reporting System

The US-CERT Incident Reporting System provides a secure web-enabled means of reporting computer security incidents to US-CERT. This system assists analysts in providing timely handling of your security incidents as well as the ability to conduct improved analysis. If you would like to report a computer security incident, please complete the following form. + More Detail

Section: Reporter's Contact Information

First Name *(Required)*	
Last Name *(Required)*	
Email Address *(Required)*	
Telephone number *(Required)*	
Are you reporting as part of an Information Sharing and Analysis Center (ISAC)?	No, this is not an ISAC report
What type of organization is reporting this incident? *(Required)*	Please select
What is the impact to the reporting organization? *(Required)*	Please select
What type of followup action are you requesting at this time? *(Required)*	Please select
Describe the current status or resolution of this incident. *(Required)*	Please select
From what time zone are you making this report? *(Required)*	Please select a time zone
What is the approx time the incident started? (local time)	September 12 . 2013 : 19 : 41
When was this incident detected? (local time)	September 12 . 2013 : 19 : 41

Multi-State ISAC

Multi-State Information Sharing and Analysis Center

- Membership includes all 50 States and over 1000 local government organizations, U.S. territories and tribal nations
- Supports CS&C's efforts to secure cyberspace by disseminating early warnings of cyber threats to SLTT governments
- Shares security incident information and analysis
- Runs a 24-hour watch and warning security operations center
- Provides Albert II Intrusion Detection

MS-ISAC

How to Report a Suspected Incident:

If there is a suspected or confirmed cyber incident that:

- Affects core government functions;
- Affects critical infrastructure functions;
- Results in the loss of data, system availability; or control of systems; or
- Indicates malicious software is present on critical systems.

The Multi-State Information Sharing and Analysis Center (MS-ISAC):

Call: (866) 787-4722
Email: soc@msisac.org

Cyber Security Advisors (CSA) & Protective Security Advisors (PSA)

- Regionally-based DHS personnel
- Direct coordination to bolster the cybersecurity preparedness, risk mitigation, and incident response capabilities of SLTT governments and private sector critical infrastructure entities at no-cost
- Provide actionable information and able to 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
- Available to assist with planning and incident management assistance for both cyber and physical incidents
- Currently 8 CSAs and ~100 PSAs

Summary of Services

Needs	DHS Services	Summary
Vulnerability Identification and Mitigation	Cyber Hygiene Scanning	Automated scans of internet facing systems: • Configuration error • Vulnerability scanning
	Risk and Vulnerability Assessment	• Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
Information Sharing	NCCIC Alerts	Provides support and expertise to critical infrastructure owners and operators, and SLTT governments.
	MS-ISAC	Provides advisories, newsletters, cybersecurity guides and toolkits from the central resource for situational awareness and incident response for SLTT
Local, In-Person Support	Cyber Security Advisors Protective Security Advisors	Regionally located personnel that provide immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats.
Incident Response	NCCIC	The Federal Government's 24x7 cyber situational awareness, incident response, and management center.
	MS-ISAC	24x7 Security Operations Center serving as a central resource for situational awareness and incident response for SLTT governments.

For more information email SLTTCyber@hq.dhs.gov

Election Infrastructure

Election infrastructure represents the assets, systems, and networks most critical to the security and resilience of the election process, which includes:

- **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 State and localities to process absentee and Election Day voting materials
- 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

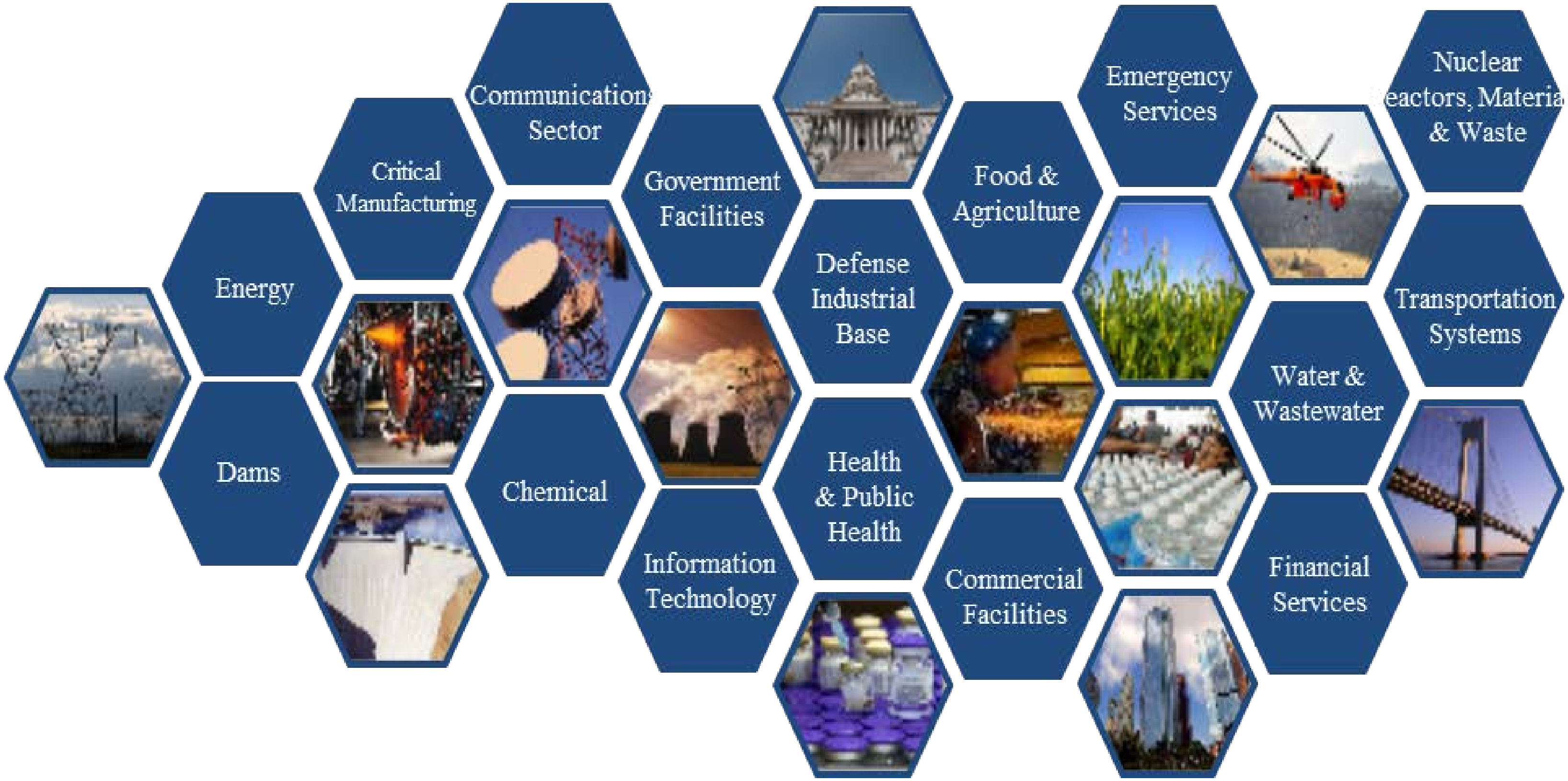
Election Infrastructure as Critical Infrastructure

- Definition of Critical Infrastructure
  - "Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

- DHS has determined that systems and assets included in election infrastructure meet this definition of critical infrastructure

- On January 6, 2017, Secretary Jeh Johnson established election infrastructure as a critical infrastructure sub-sector of the existing government facilities sector
  - Secretary Johnson identified DHS's National Protection and Programs Directorate as the sector specific agency for the election infrastructure sub-sector

Designation of Critical Infrastructure Sectors



- Energy
- Dams
- Critical Manufacturing
- Communications Sector
- Chemical
- Government Facilities
- Information Technology
- Defense Industrial Base
- Health & Public Health
- Food & Agriculture
- Commercial Facilities
- Emergency Services
- Water & Wastewater
- Financial Services
- Nuclear Reactors, Materials & Waste
- Transportation Systems

Benefits of Designation – Reduce System Vulnerabilities

In addition to the services already discussed…

- Designation as a sub-sector establishes mechanisms to rapidly share information across the community to identify and mitigate system vulnerabilities

- Coordinating councils will be established, focused on the physical and cyber security and resilience of the election infrastructure
  - Coordinating councils are used to share information on vulnerabilities and threats and to enable collaboration across Federal, state, and local governments, as well as with private sector partners, to determine ways to mitigate risks
  - Participation in the council is voluntary
  - Coordinating Councils are used widely by the private sector critical infrastructure community (Energy SCC, FS-SCC, IT-SCC, etc)

Benefits of Designation – Reduce System Vulnerabilities (cont)

- Critical Infrastructure Partnership Advisory Council (CIPAC) protections
  - Allows sector coordinating councils to include private vendors and experts from information technology firms to actively participate in sensitive security conversations and planning alongside their government partners
  - This would provide election officials with greater access to a broad range of technical and security expertise

- Protected Critical Infrastructure Information (PCII)
  - Operators of critical infrastructure can voluntarily share information with DHS via PCII to exempt that information's dissemination in Freedom of Information Act (FOIA) requests, use in civil litigation, and regulatory use
  - States, vendors, or individuals that identify vulnerabilities in election infrastructure can share this information, to the benefit of all who leverage these systems, without fear that it will be used against them
  - Provides an effective mechanism for election officials to share vulnerability information and ensure that mitigations can be applied by all

Benefits of Designation – Understand Threats to Election Infrastructure

In addition to the services already discussed…

- Designation as a subsector allows DHS to provide security clearances to election officials, as appropriate.
  - Election officials could be briefed on relevant classified intelligence and leverage that to secure their systems in a manner more informed of the threats they face

Benefits of Designation – Respond to Incidents and Malicious Cyber Actors

In addition to the services already discussed…

- Designation as a sub-sector allows owners and operators of election infrastructure to benefit from the U.S. government's strategic and policy-based efforts to protect critical infrastructure
  - Promotion of international norms that prohibit peacetime cyber attacks against critical infrastructure
  - Use of Executive Orders to respond to attacks on critical infrastructure

Executive Order 13964

- As a sub-sector of critical infrastructure, the Secretary of Treasury is able to sanction persons responsible for cyber enabled activities that harm or compromise a computer that supports an entity in a critical infrastructure sector
  - This would cover malicious cyber attacks that, for example, deleted data, impaired the function of a system, or destroyed a system

- On 29 December 2016, EO 13694 was amended to enable the Secretary of Treasury to also sanction persons responsible for cyber enabled activities that tamper with, alter, or cause a misappropriation of information with the purpose or effect of interfering with or undermining election processes or institutions
- These protections may serve to deter future malicious cyber behaviors or allow the U.S. government to hold cyber actors accountable for their actions.

Q&A

SLTTCyber@hq.dhs.gov

Homeland Security

Fact Sheet: Designation of Election Infrastructure as Critical Infrastructure

Consistent with Presidential Policy Directive (PPD) 21, the Secretary of Homeland Security has established Election Infrastructure as a critical infrastructure subsector within the Government Facilities Sector.

Election infrastructure includes a diverse set of assets, systems, and networks critical to the administration of the election process. When we use the term “election infrastrucure,” we mean the 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. Specficially, we mean at least 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.

Components of election infrastructure include, but are not limited to:

- 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.

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.

January 2017

Press Office
U.S. Department of Homeland Security

Press Release

January 6, 2017

STATEMENT BY SECRETARY JEH JOHNSON ON THE DESIGNATION OF ELECTION INFRASTRUCTURE AS A CRITICAL INFRASTRUCTURE SUBSECTOR

I have determined that election infrastructure in this country should be designated as a subsector of the existing Government Facilities critical infrastructure sector. Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law.

I have reached this determination so that election infrastructure will, on a more formal and enduring basis, be a priority for cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By “election infrastructure,” we mean storage facilities, polling places, and centralized vote tabulations locations used to support the election process, and information and communications technology to include voter registration databases, voting machines, and other systems to manage the election process and report and display results on behalf of state and local governments.

Prior to reaching this determination, my staff and I consulted many state and local election officials; I am aware that many of them are opposed to this designation. It is important to stress what this designation does and does not mean. This designation does not mean a federal takeover, regulation, oversight or intrusion concerning elections in this country. This designation does nothing to change the role state and local governments have in administering and running elections.

The designation of election infrastructure as critical infrastructure subsector does mean that election infrastructure becomes a priority within the National Infrastructure Protection Plan. It also enables this Department to prioritize our cybersecurity assistance to state and local election officials, but only for those who request it. Further, the designation makes clear both domestically and internationally that election infrastructure enjoys all the benefits and protections of critical infrastructure that the U.S. government has to offer. Finally, a designation makes it easier for the federal government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information.

Particularly in these times, this designation is simply the right and obvious thing to do.

At present, there are sixteen critical infrastructure sectors, including twenty subsectors that are eligible to receive prioritized cybersecurity assistance from the Department of Homeland Security. The existing critical infrastructure sectors are:

Chemical
Commercial Facilities
Communications
Critical Manufacturing
Dams
Defense Industrial Base
Emergency Services
Energy
Financial Services
Food and Agriculture
Government Facilities
Healthcare and Public Health
Information Technology
Nuclear Reactors, Material, and Waste
Transportation Systems
Water and Wastewater Systems

Entities within these sectors all benefit from this designation and work with us closely on cybersecurity. For example, we have developed joint cybersecurity exercises with numerous companies within the communications, information technology, financial services and energy sectors to improve our incident response capabilities. We have also streamlined access to unclassified and classified information to critical infrastructure owners and operators in partnership with information sharing and analysis organizations. Moreover, many critical infrastructure sectors include assets and systems owned and operated by state and local governments, such as dams, healthcare and public health, and water and wastewater systems.

Now more than ever, it is important that we offer our assistance to state and local election officials in the cybersecurity of their systems. Election infrastructure is vital to our national interests, and cyber attacks on this country are becoming more sophisticated, and bad cyber actors – ranging from nation states, cyber criminals and hacktivists – are becoming more sophisticated and dangerous.

Further, our increasingly digital and connected world has reshaped our lives. It has streamlined everyday tasks and changed the way we communicate. But, just as the continually evolving digital age has improved our quality of life, it has also introduced an array of cyber threats and implications.

Cybersecurity continues to be a top priority for DHS, as it is for state and local election officials across the country. This designation enables the states, should they request it, to leverage the full scope of cybersecurity services we can make available to them.

###