

MEMORANDUM FOR: Suzanne E. Spaulding
Under Secretary for National Protection and Programs
Directorate

FROM: Jeh Charles Johnson

SUBJECT: Designation of Election Infrastructure as a Subsector of the
Government Facilities Critical Infrastructure Sector

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, certain systems and assets of election infrastructure meet the statutory definition of critical infrastructure in fact and in law.

I have reached this determination so that election infrastructure, on a more formal and enduring basis, continues to be a priority in the cybersecurity assistance and protections that the Department of Homeland Security provides to a range of private and public sector entities. By "election infrastructure," I 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. 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.

I direct the National Protection and Programs Directorate (NPPD) to institutionalize the Election Infrastructure subsector in the Government Facilities sector under the National Infrastructure and Protection Plan (NIPP) and incorporate the subsector into the NIPP framework. An NPPD serves as a Sector Specific Agency for the Government Facilities sector, I also direct NPPD to serve as the Sector Specific Agency for the Election Infrastructure subsector on behalf of DHS.

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. This designation enables the states, should they request it, to leverage the full scope of cybersecurity services available to them.

- **Election Infrastructure Subsector Q&As**

Q: What is the process by which DHS establishes a critical infrastructure sector?

- Presidential Policy Directive 21: *Critical Infrastructure Security and Resilience* directs the Secretary of Homeland Security to evaluate the need for, and approve changes to, critical infrastructure sectors. The only requirement in this process is that the Secretary shall consult with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated Sector-Specific Agency for that sector. The term "critical infrastructure" has the meaning provided in section 1016(e) of the USA Patriot Act of 2001 (42 U.S.C. 5195c(e)), namely 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.

Q: Can this decision be reversed by the next Administration?

- Future Administrations may outline similar authorities regarding the structure and organization of critical infrastructure sectors, however, unless amended, the definition of "critical infrastructure" will remain as provided in the USA Patriot Act of 2001, as amended.
- Designations of critical infrastructure sectors are addressed in Presidential Policy Directive 21. Future Administrations may institute their own policy directives.
- We note that Administrations often choose to leave policy directives from previous administrations in place and update them as needed. For example, PPD-21, signed February 2013, replaced Homeland Security Presidential Directive 7 (Critical Infrastructure Identification, Prioritization, and Protection), issued in December 2003. DHS's Critical Infrastructure work spans administrations, pre-dating the Department with the Clinton administration, becoming formalized under the George W. Bush administration, then adapted and updated by the Obama administration.

Q: Are there any carve-outs or safe harbors that states could employ to exempt them from a designation?

- All participation, including receipt of services and engagements with sector coordinating council is entirely voluntary.

Q: What would establishing a critical infrastructure sector or subsector mean for the elections community?

- First, it is important to note that **all participation is entirely voluntary** in any of the offerings for critical infrastructure stakeholders. If your state or jurisdiction does not want to leverage any of the services or benefits DHS provides to the critical infrastructure community, DHS will not compel you to do so. Establishing a critical infrastructure subsector for elections **does not involve Federal intrusion, takeover, or regulation** of any kind. Rather, establishment provides the benefit of certain protections and services that are voluntary and upon request.
- Second, the existing technical assistance services that several states are taking advantage of will continue. These include the following services for which states have reported very positive feedback:
 - **Cyber Hygiene scans on Internet-facing systems:** These scans can provide election officials with a report identifying vulnerabilities and mitigation recommendations to improve their cybersecurity posture, and
 - **Risk and Vulnerability Assessments (RVAs):** These assessments include a wide range of penetration testing services, application, and database testing.
- Establishment of election infrastructure as a critical infrastructure subsector would enable DHS to prioritize its assistance to election officials in three phases:
 1. Reduce system vulnerabilities
 2. Understand threats to election infrastructure
 3. Respond to incidents and malicious cyber actors

Reduce system vulnerabilities

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

1. Designation as a sub-sector would support the establishment of a **sector coordinating council** focused on the 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.
2. A sub-sector would be covered by the **Critical Infrastructure Partnership Advisory Council (CIPAC)** framework, so that DHS could convene meetings with state and local election officials, and these meetings could be closed to the public and exempt from FACA requirements.

Order 13694 would be able to sanction persons responsible for cyber enabled activities that harm or compromise a computer that supports an entity in a critical infrastructure sector.

Last month, this Executive Order was amended to enable the Secretary of Treasury to also be able to 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. This amendment was added because of Russian activities related to the 2016 U.S. election. Establishing a sub-sector for election infrastructure would enable the Executive Order to be used against actors that intend to harm or compromise election systems more broadly, including for theft of personal information involving a computer that supports an entity in a critical infrastructure sector, for example, that undermines confidence in the confidentiality of voter registration databases and, thereby, may lead to lower the public's willingness to register. These protections may serve to deter future malicious cyber behaviors or allow the U.S. government to hold cyber actors accountable for their actions.

3. **Protected Critical Infrastructure Information (PCII).** Additionally, developers and operators of infrastructure can voluntarily share critical information with DHS under a **protection of critical infrastructure information (PCII)** statute that protects information from Freedom of Information Act (FOIA) requests, use in civil litigation, and regulatory use.¹ In practice, this means that 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. This, in combination with the heightened awareness of vulnerabilities through the sector coordinating council, provides an effective mechanism for a state that learns of and remediates a vulnerability to take steps to ensure that their mitigation solution can be applied to all other states and localities impacted by the same vulnerability.

Understand threats to election infrastructure

Additionally, as a critical infrastructure subsector, DHS would be able to prioritize providing **security clearances to election officials** as appropriate. This would enable election officials to be briefed on relevant classified intelligence, and to secure their systems in a manner more informed of the threats they face. In other sectors, this type of information is especially valuable in the engineering, design, and procurement decisions among the sector.

Respond to incidents and malicious cyber actors

DHS provides funding for the Multi-State Information Sharing and Analysis Center (MS-ISAC). States already have access to the **cyber incident response capabilities of the MS-ISAC**, however, historically, much of the MS-ISAC's attention has focused on the work of the Chief Information Officers and Chief Information Security Officers for each state's overall systems and networks. As a critical infrastructure subsector, election officials' incident response needs and requests for services can be prioritized, both by DHS and MS-ISAC, over requests from non-critical infrastructure stakeholders.

- Lastly, owners and operators of election infrastructure in a designated subsector would benefit from the U.S. government's **strategic efforts to protect critical infrastructure**, including the promotion of **international norms that prohibit peacetime cyber attacks** against critical infrastructure as well as the use of certain **Executive Orders to respond to attacks** on election infrastructure. As a sub-sector of critical infrastructure, the Secretary of Treasury, under Executive

¹ See 6 U.S.C. §133

TICK TOCK:

Friday, January 6: This guidance is shared under embargo with DOJ, FBI and NIST.

Following the release of the IC report:

- + 2 hours; NASS and Congressional leadership staff notifications
- +2.30 hours; OLA notifications to Authorizers and Appropriators
- + 2:45 hours; Embargoed release to other Congressional members
- + 3 hours; Secretary Johnson issues statement
- + 3:30 hours; Stakeholder notifications




**Homeland
Security**

July 7, 2017

ACTION MEMORANDUM

MEMORANDUM FOR DISTRIBUTION

FROM: Bob Kolasky 
Deputy Under Secretary (Acting)

TO: A/ S, Office of Infrastructure Protection
DU/S (A), Cybersecurity and Communications
Director, Office of Cyber and Infrastructure Analysis

Cc: U/S, Office of Intelligence & Analysis

SUBJECT: **Election Infrastructure Subsector Formation Action Plan**

Purpose: To promulgate the Election Infrastructure Action Plan for forming the Election Infrastructure Subsector.

Background: In January 2017, Secretary Jeh Johnson designated the nation's election infrastructure as a subsector of the Government Facilities Sector. Secretary John Kelly affirmed this subsector designation.

The National Protection and Programs Directorate has been designated as the Election Infrastructure Sector Specific Agency (SSA).

The attached Action Plan lays out actions to implement and establish the Election Infrastructure Subsector. This plan outlines five "Lines of Effort" (LOEs) with the overarching goals of defining the scope and elements of the subsector, implementing an immediate information sharing and notification capability, developing an architecture for governance of the subsector, further establishing cybersecurity support, and implementing an External Affairs strategy to ensure broad understanding and gain support for this effort.

Action: All NPPD offices and subcomponents will support the efforts listed in the Action Plan. The intent of this effort is to assist state and local government election officials and private election infrastructure vendors and stakeholders in ensuring the security and integrity of the election infrastructure subsector.

Assigned Line of Effort (LOE) leads are responsible for coordinating all actions under each LOE.

LOE leads are as follows:

- LOE 1: Define the Subsector. Lead: OCIA, in coordination with IP
- LOE 2: Establish Information Sharing Processes, Protocols, and Architectures. Lead: IP, in coordination with CS&C.
- LOE 3: Develop Subsector NIPP Framework and Governance. Lead: IP
- LOE 4: Cyber security Support. Lead: CS&C
- LOE 5: External Affairs. Lead: NPPD/External Affairs

A table listing leads for each task within the LOEs is provided at the end of the Plan.

It is important that DHS expeditiously stand up initial subsector capabilities to meet the intent prior to the fall 2017 election cycle.

This plan is intended as a framework and will be adjusted as needed. An NPPD enterprise-wide approach in this effort is essential. Your contributions and teamwork in this important effort are appreciated.

Attachment:

Election Infrastructure Subsector Formation Action Plan - FINAL – 5 July 2017

Distribution:

David Hess, Senior Official Performing the Duties of Under Secretary
Steven Harris, Chief of Staff (Acting)
Daniel Ahr, Deputy Chief of Staff (Acting)
Danny Toler, Assistant Secretary, Office of Cybersecurity and Communications (Acting)
L. Eric Patterson, Director, Federal Protective Service
David Wulf, Deputy Assistant Secretary, Office of Infrastructure Protection (Acting)
Shonnie Lyon, Director, Office of Biometric Identity Management
Brandon Wales, Director, Office of Cyber and Infrastructure Analysis
Ernie Robinson, Director, External Affairs
Jeanette Manfra, Deputy Under Secretary for Cybersecurity and Communications
Emily Early, Director, Strategy, Policy, and Plans (Acting)
Jonathan Carver, Chief Financial Officer
Nicole Windham, Director, Management
Daniel Sutherland, Associate General Counsel

Election Infrastructure Subsector Formation

Action Plan

FINAL – July 5, 2017

OVERVIEW AND PURPOSE

Following Secretary Jeh Johnson’s designation of the nation’s elections systems as a critical infrastructure subsector, and Secretary John Kelly’s subsequent affirmation of this designation, this plan lays out actions to implement and establish the Election Infrastructure Subsector (under the Government Facilities Sector). This plan outlines five lines of effort with the overarching goals of defining the scope and elements of the subsector, implementing an immediate information sharing and notification capability, developing an architecture for governance of the subsector, and implementing an External Affairs strategy to ensure broad understanding and gain support for this effort.

THREAT ASSESSMENT

Multiple elements of U.S. election infrastructure are potentially vulnerable to cyber intrusions. The risk to U.S. computer-enabled election systems varies from county to county, between types of devices used, and among processes used by polling stations.ⁱ

RESPONSIBILITIES

DHS, as represented by the National Protection and Programs Directorate (NPPD) Office of Infrastructure Protection (IP) was assigned as the lead for SSA management responsibilities on behalf of DHS. (Note: The Election Infrastructure Subsector is a subsector under the Government Facilities Sector, of which DHS NPPD/Federal Protective Service (FPS) and GSA are co-leads). Other parts of NPPD have critical roles in helping secure election infrastructure – most prominently the Office of Cyber Security and Communications (CS&C) and the Office of Cyber and Infrastructure Analysis (OCIA). NPPD subcomponents will work together to support the sector guided by this plan.

INTENT

The intent of this effort is to assist state and local government election officials and private election infrastructure vendors in ensuring the security and integrity of the election infrastructure.

Key aspects of this intent are to enhance subsector physical and cyber security to ensure the confidentiality (people’s votes aren’t revealed and personally identifiable information (PII) is not compromised), integrity (votes and databases aren’t manipulated), and availability (databases and systems are available when needed) of election infrastructure.

STRATEGIC OBJECTIVES

1. Expeditiously stand up initial subsector capabilities to meet the intent prior to the fall 2017 election cycle.
2. Establish a robust communications, notification, and information sharing capability between election infrastructure stakeholders at the Federal, State, and local level, to include vendors, when appropriate.
3. Establish an appropriate representational organizational structure that fully represents all appropriate stakeholders.

4. Establish enduring, trusted relationships with subsector stakeholders.
5. Communicate information regarding proposed, ongoing, and upcoming actions as the subsector stands up, and support the development of trust-based relationships with this unique audience by ensuring potential stakeholders are aware, informed, and engaged.

CONCEPT OF OPERATIONS

Activities to establish the subsector, to include development of council structure, will occur **concurrently** with the development and implementation of an architecture, mechanisms, and procedures for notification and information sharing. DHS recognizes the need for near-term information sharing capabilities is a top priority.

IP, in close coordination with CS&C, OCIA, and NPPD Strategy, Policy, and Plans (SPP), will perform the duties in line with the National Infrastructure Protection Plan (NIPP) to lead and coordinate subsector establishment activities. These activities include stakeholder outreach, executive secretariat support, planning efforts, development of sector governance documents and limited technical assistance efforts. IP should coordinate with representatives from each of the major non-federal government entities in this effort.

CS&C will actively participate in stakeholder outreach efforts and provide technical assistance on cybersecurity vulnerabilities and cyber-related issues.

OCIA will actively support the development of analytical products intended to provide a foundational understanding of the sub-sector and its risk landscape. This will assist sector partners in establishing goals, objectives, and key priority activities for the new sub-sector.

The NPPD Federal Protective Service (FPS) and the General Service Administration (GSA) will continue as co-chairs for the Government Facilities sectors but will not have any formal responsibilities for the Election Infrastructure Subsector. IP, representing DHS as the Subsector SSA, will provide periodic written updates to the Government Facilities Sector SSAs for communications purposes.

The base date for actions in this plan is 5 July 2017.

GOVERNANCE / TASK ORGANIZATION

IP will serve as the NPPD lead for this Action Plan, and will assign a single Plan Coordinator to oversee the implementation of the plan. IP will coordinate with CS&C, OCIA, and Strategy, Policy and Plans (SPP) in this effort. IP shall coordinate with sector stakeholders, as appropriate.

Leads for each Line of Effort are listed below, and will report progress to the Under Secretary and Deputy Under Secretary through the Plan Coordinator.

Leads for each specific task are listed in the table at the end of this document. (Attachment 1)

LINES OF EFFORT (LOEs) AND ACTIONS

There are five LOEs:

1. Define the subsector
2. Establish Information Sharing Processes, Protocols, and Architectures
3. Develop Subsector Councils Structure and Governance
4. Cybersecurity Support
5. External Affairs

LOE 1: Define the Subsector

LEAD: OCIA in coordination with IP

Goal: Develop a definition of the subsector that incorporates the appropriate elements that encompass the subsector, to include election officials, associations, and manufacturers of equipment, voter databases, systems, networks, and assets for voting, recording, and tabulating results.

Tasks:

1. Determine Scope and develop definition of the subsector. Incorporate the appropriate elements that encompass the subsector, consider the following: **(14 Days)**
 - a. Assets, systems, networks
 - b. Equipment
 - c. Databases
2. Provide an overview of the primary federal laws and authorities affecting U.S. elections and how NPPD fits into the election landscape to include NPPD's cyber authorities. **(7 days)**
3. Identify comprehensive list of types of stakeholders **(14 Days)**
 - a. Owners/ operators: Election officials (at State and local level)
 - b. Associations: National Association of Secretaries of State, National Association of State Election Directors, National Association of Counties, etc.
 - c. Vendors and manufacturers of equipment
4. Identify other existing organizations and associations that represent identified stakeholders. **(14 Days)**
 - a. IP should coordinate with NPPD External Affairs and the DHS Office of Public Engagement / State and Local Affairs on this effort.
 - b. Develop concept for working with party organizations, campaigns, and related entities that are integral to elections but not necessarily part of election infrastructure
5. Conduct Risk Assessments
 - a. Conduct risk assessment for States with 2017 major elections **(60 Days)**
 - b. Conduct subsector risk assessment **(180 days)**

LOE 2: Establish Information Sharing Processes, Protocols, and Architectures

LEAD: IP, in coordination with CS&C.

Goal: Establish mechanisms for swift communication and information sharing. Prioritize States with 2017 major election activities.

Tasks:

1. Establish an outreach and engagement plan to ensure awareness of sector formation activities by appropriate stakeholders **(7 days)**
2. Establish a deliberate (routine) and incident notification protocols and supporting processes:
 - a. NICC Notifications **(14 Days)**
 - b. NCCIC Notifications **(14 Days)**
 - c. Develop Notification Listserves of stakeholders, define when and how they would be used, and establish protocols for dissemination of information. **(14 Days)**
 - i. Secs of state
 - ii. Election Directors
 - iii. NASS
 - iv. EAC
 - v. Election Infrastructure Vendors
 - vi. TBD
3. HSIN. Establish HSIN Elections Infrastructure Community of Interest (COI) site and nomination and validation procedures. **(21 Days)**
4. Establish/ Identify Information Sharing and analysis responsibilities (ISAC/ISAO) for Elections Infrastructure Subsector ISAC/ISAO **(21 Days)**
 - a. Leverage or establish capability similar to MS-ISAC for SLTT component of elections infrastructure
 - b. Identify and or establish ISAC/ISAO functions for elections vendor community
 - c. Determine funding source and requirements
 - i. Consider leveraging existing Federally funded ISACs (Comms ISAC, MS-ISAC)
5. Establish an interim subsector incident response playbook, outlining roles and responsibilities between Federal government, SLTT election officials and other entities, and vendors of election infrastructure during an incident **(45 Days)**
 - a. Incorporate physical and cyber incidents
 - b. Include options for public messaging and emphasize USG support to election officials
6. Security Clearances – Establish process, criteria, and point of contact for security clearance for appropriate stakeholders. **(45 Days)**

7. Exercise Info Sharing Protocols and Incident Management – Working through established council structures (see LOE 3), test info sharing protocols, and incident response playbook via an inclusive exercise **(150 Days)**

LOE 3: Develop Subsector NIPP Framework and Governance

LEAD: IP

Goal: Establish a governance structure for representation of Federal and non-Federal government officials and appropriate private sector entities. The structure will include the following:

Overview:

Subsector governance will be in accordance with the NIPP framework, as developed under Presidential Policy Directive 21 (PPD-21) *Critical Infrastructure Security and Resilience*. Activities of the Subsector will be guided by the Critical Infrastructure Partnership Advisory Council (CIPAC) structure, which facilitates interaction between governmental entities and representatives from private sector critical infrastructure entities. CIPAC provides a forum in which the government and private sector entities, organized as coordinating councils, can jointly engage in a broad spectrum of activities to support and coordinate critical infrastructure security and resilience efforts.

Elections Infrastructure Government Coordinating Council (EI GCC). The EI GCC will be formed to enable interagency and cross-jurisdictional coordination. The GCC will be composed of representatives from across the Federal, State, and local levels of government. The GCC must be representative of the broad government stakeholder community for state and local election entities who will interact on a wide range of sector-specific strategies, policies, activities, and issues. The GCC serves as the principal collaboration point between government and private sector stakeholders for critical infrastructure security and resilience policy coordination. The GCC will have an Executive Committee which will include DHS, the Elections Advisory Commission (EAC) and other key entities which will guide GCC activities.

Election Infrastructure Sector Coordinating Council (EI SCC). The EI SCC will be a self-organized, self-run, and self-governed private sector council consisting of private sector owners and operators and their representatives, which interact on a wide range of sector-specific strategies, policies, activities, and issues. The SCC will serve as the principal collaboration point between the government and private sector owners and operators of Election Infrastructure.

Tasks:

1. Propose the Government Coordinating Council Structure to DHS Leadership for Approval **(14 Days)**
2. Identify government organizations for membership on GCC **(21 Days)**
 - a. Coordinate partnership meeting engagements, for interested parties.
 - b. Collaborate with EAC on membership
 - c. Determine appropriate roles for NASS, NASED, and NACo.

3. Develop and provide initial draft charters for further refinement development by the prospective Government Coordinating Council (GCC) and Sector Coordinating Councils (SCC) **(28 Days)**
4. In coordination with SSA Leadership, Identify Executive Committee for the GCC **(30 Days)**
5. Establish an EI SSA Management Office to coordinate subsector structural and governance development. **(30 Days)**
 - a. EI SSA Management Office should focus and take action on initial partnership issues/questions (security clearance process/quotas, intelligence sharing, cybersecurity priorities, etc.).
Perform other actions as required to establish a robust, enduring subsector partnership and information sharing capability.
6. Establish GCC **(60 Days)**
 - a. Develop initial charter
 - b. Solicit membership of interested parties
 - c. Hold engagement sessions to further NIPP partnership education
7. Facilitate Development of SCC **(90 Days)**
 - a. Develop initial charter
 - b. Solicit membership of interested parties
 - c. Hold engagement sessions to further NIPP partnership education
8. Establish CIPAC Working Groups to address immediate priorities **(90 days)**
 - a. Use this key capability to take on imminent and/or pressing issues
 - b. Establish appropriate WGs such as Information Sharing WG, Cybersecurity WG, etc., or specific TFs such as Fall 2017 Election (VA and NJ focused) Task Force.
9. Develop interim Sector Specific Plan (SSP) with goals, objectives, and priorities **(120 Days)**
10. Identify, via SSA Management Office, CIPAC secretariat support **(45 days)**

LOE 4: Cyber security Support

LEAD: CS&C

Goal: Develop and implement protocols, activities, and processes and provide near-term prioritized cybersecurity support to the Election Infrastructure Subsector stakeholders. Develop sustaining protocols, activities, and processes.

Tasks:

1. Establish an EI Cybersecurity Working Group to understand operational requirements and address immediate risks. The working group will seek to develop a comprehensive understanding of the operational requirements and formulate scalable methodology to provide technical services/support to address cyber risks **(30 Days)**

- a. Establish coordination between WG and MS-ISAC (or other appropriate entity) to scope level and content for elections support.
2. Provide an overview of CS&C capabilities and offerings for SLTT as well as define the technical services the NCCIC can offer states in the election context. **(7 Days)**
3. Establish content and format expectations for reporting cybersecurity incidents and sharing network protection information as part of overall info sharing protocols. **(30 Days)**
4. Determine prioritization schema for allocation of resources for election infrastructure requests for services/ technical assistance, focused on cyber security support but applicable to physical security support as well **(60 Days)**
5. Establish plan for election day (vote casting period) operational coordination and support **(90 Days)**

LOE 5: External Affairs

Lead: External Affairs

Goal: Develop and implement a comprehensive External Affairs plan to keep key audiences informed of actions being taken by DHS in support of joint efforts to establish an election subsector – including potential subsector members and the organizations that represent them, members of Congress, and the media; promote understanding of DHS’ role in this effort and the benefits offered through the sector structure; and help secure buy-in from these audiences.

Overview:

Securing our hometowns and our nation against the many threats we face is a task that requires all of us to work together - public, private, state, local, tribal, territorial, and federal. Under the National Infrastructure Protection Plan (NIPP), one role the Department of Homeland Security plays is to provide technical assistance and other tools in support of government and private sector partners at the state, local, tribal, and territorial levels as they work to secure their own infrastructure.

Tasks:

1. Draft an external affairs strategy that leverages public affairs, legislative affairs, public engagement and strategic communications support in a comprehensive and integrated approach. **(7 days)**
2. Establish a schedule of anticipated outreach activities and update with opportunistic efforts, such as press releases, blogs, speaking opportunities and other proactive outreach. **(7 days)**
3. Identify resources from across NPPD to support implementation of the external affairs strategy. **(10 days)**

4. Develop core messaging, FAQs, media toolkits, visual aids and other outreach materials as required, in coordination with component and working group SMEs **(10 days)**
5. Work with program lead to respond to media, legislative, and stakeholder inquiries. **(as needed)**

RISKS

1. Resources. Analysis of resource requirements is not considered in this action plan. Planning for future, long-term resource requirements is required.
2. Stakeholder Representation. Near-term action items create a risk of omitting some key stakeholders. Efforts to ensure inclusion of all stakeholder and non-dominance of a select few in the council's structure is imperative.
3. Building Trust and Relationships. Establishing trusted relationships is key to the success of the NIPP partnership model. The rapid establishment of the EI sector structure presents a challenge to creating trusted relationships. Transparency, responsiveness, and dependability are essential in this effort.
4. Environment. The subsector is highly politicized and under media scrutiny. Every effort must be made to build trusted relationships and transparency about the efforts underway in the subsector.

ATTACHMENT 1:

Lines of Effort (LOE) Task Timeline Table:

LOE Task #:	LOE Task Description	Lead	Supporting Organization(s)	Due Date
1-1	Subsector Scope/Definition	OCIA		19 July
1-2	Legal Overview	NPPD LD/OGC	EAC, DOJ	12 July
1-3	Stakeholder Analysis/Types	IP/SOPD	All	19 July
1-4 a and b	Organization/Association analysis	IP/SOPD	All	19 July
1-5a	Conduct key State assessments	OCIA	IP, CS&C	3 September
1-5b	Conduct Subsector Risk Assessment	OCIA	IP, CS&C	1 January 2018
2-1	Establish Outreach & Engagement Plan	External Affairs	IP/, CS&C	12 July
2-2a	NICC Notifications	IP/NICC	All	19 July
2-2b	NCCIC Notifications	CS&C/NCCIC	All	19 July
2-2c	Develop notification listserves	IP/SOPD-NICC & CS&C/SECIR-NCCIC	All	19 July
2-3	Establish HSIN EI COI	IP/SOPD	All	26 July
2-4	Establish ISAC/ISAO responsibilities	CS&C/IP	All	26 July
2-5	Interim Incident Response Playbook(s)	CS&C/IP	All	19 August
2-6	Establish Security Clearance Process	I&A/IP	All	19 August
2-7	Exercise Info Sharing Protocols	IP/SOPD	All	2 December
3-1	Propose Government Coordinating Council (GCC) structure	IP/SOPD & CS&C/SECIR	All	19 July
3-2	ID Government Organizations for GCC	IP/SOPD	All	26 July
3-3	Develop draft charters	IP/SOPD	All	2 August
3-4	ID Executive Committee Options	IP/SOPD and CS&C/SECIR		4 August
3-5	Establish EI SSA Management Office	IP/SOPD	All	4 August
3-6	Establish GCC	IP/SOPD & CS&C/SECIR	All	3 September

3-7	Facilitate development of SCC	IP/SOPD & CS&C/SECIR	All	3 October
3-8	Establish CIPAC/GCC Working Groups	IP/SOPD	All	3 October
3-9	Develop interim Sector Specific Plan	IP/SOPD	All	2 November
3-10	ID CIPAC Secretariat support	IP/SOPD	All	19 August
4-1	Establish EI Cybersecurity WG	CS&C/SECIR	All	4 August
4-2	Provide overview of CS&C capabilities	CS&C/EPMO	All	12 July
4-3	Establish cyber IM reporting formats/+	CS&C/NCCIC	All	4 August
4-4	Determine prioritization schema for cyber resources	CS&C	All	3 September
4-5	Establish “Election Day” cyber support plan	CS&C	All	3 October
5-1	Draft External Affairs Strategy	External Affairs	All	12 July
5-2	Establish a schedule of outreach activities	External Affairs	All	12 July
5-3	ID NPPD EI External Affairs resources	External Affairs	IP, CS&C	15 July
5-4	Develop core messaging, FAQs, etc.	External Affairs	IP, CS&C	15 July
5-5	Coordinate plan for responses to media, legislative, and stakeholder inquiries	External Affairs	IP, CS&C	(as needed)

ⁱ (U//FOUO) Cyber Threats and Vulnerabilities to US Election Infrastructure; DHS Office of Intelligence and Analysis IA-0213—16, 20 Sep 2016

Critical Infrastructure Designation Tick Tock:

Thursday, January 5

- 2:45 pm: Call with National Association of Secretaries of State Working Group Members & EAC Commissioners
- 3:45: National Association of Counties & National Association of County Recorders, Election Officials & Clerks

Friday, January 6

- 9:15 am: Embargoed OLA notifications
- 9:30 am: Secretary Johnson issues statement
- 9:30 am: Stakeholder message



Homeland
Security

August 3, 2017

ACTION MEMORANDUM

MEMORANDUM FOR DISTRIBUTION

FROM: Bob Kolasky
(Acting) Deputy Under Secretary *BK*

THROUGH: Scott Breor, Director, Protective Security Coordination Division

TO: IP Regional Directors

CC: Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications

SUBJECT: NPPD Field-based Engagement with State Chief Election Officials

Purpose: To promulgate guidance for Office of Infrastructure Protection (IP) Regional Directors to engage with their respective state Chief Election Official, normally the Secretary of State, in order to ensure awareness of the NPPD capabilities and to better understand the Chief Election Official's (CEO) election infrastructure related needs.

Background: In January 2017, the Department designated the Nation's Election Infrastructure as a subsector of the Government Facilities Sector. Secretary Kelly affirmed this subsector designation. The National Protection and Programs Directorate (NPPD) has been designated as the Election Infrastructure Sector Specific Agency (SSA). The SSA lead role has been delegated to IP, with the Sector Outreach and Programs Division (SOPD) executing the corresponding SSA management responsibilities.

Action: NPPD is energizing all available resources to support the development of this important subsector and its key stakeholders. An NPPD enterprise-wide approach in this emergent effort is essential for sustained progress. Your direct engagement is needed to ensure broad understanding and gain support for this emerging subsector development effort.

As such, I am directing that each IP Regional Director make themselves available to meet with State's Chief Election Officials to ensure the CEO is familiar with the capabilities and resources of the IP Regional Team and that you, as Regional Director, better understand the specific election-related needs of the States within your region. Please do so in coordination with locally-based

Cyber Security Advisors in your region and any Protective Security Advisors who will have ongoing responsibility for working with Election officials.

In order to help prepare you for these meetings, the Election Infrastructure SSA team will send you a set of talking points, relevant NPPD assistance, and a listing of State Chief Election Officials by Friday, August 4 2017. Once talking points are received, these engagements should take place over the next 60 days with after-action reports, compiled via PSCD, sent back to me with copy to Juan Figueroa, who leads the Election Infrastructure SSA team.

Timeliness: Please ensure engagement completion across all ten regions and submittal of the corresponding after-action reports by Tuesday, October 3, 2017.

Distribution:

- A. IP Regional Directors (Regions I-X)
- B. David Wulf, Deputy Assistant Secretary, Office of Infrastructure Protection (Acting)
- C. Steven Nider, Chief of Staff (Acting)
- D. Linda Solheim, Director, Sector Outreach and Programs Division
- E. Danny Toler, Deputy Assistant Secretary, Office of Cybersecurity and Communications
- F. Brad Tenney, Acting Director, Stakeholder Engagement and Cyber Infrastructure Resilience
- G. Brandon Wales, Director Office of Cyber and Infrastructure Analysis

NPPD Field-Based Engagement with State Chief Election Officials

Background

- Federal, state and local officials, and the private sector all have a role to play in protecting the election subsector from the variety of threats to our critical infrastructure.
- The designation of election infrastructure as critical infrastructure does not change the primary role state and local governments have in administering and running elections, it does not create new regulations, and it does not give DHS new powers to intervene.
- Many state and local election organizations have been doing excellent work already to secure the election systems, and we believe that we can bring additional value to this effort, on an as-requested basis.

Discussion Guide

- **[Introduce yourself and mention that you are following up on conversations that have been initiated between state election officials and DHS headquarters.]**
- **[Explain your role as the Regional Director and acknowledge that the election official may also have heard from a cyber advisor, but you are part of the same team under the National Protection and Programs Directorate.]**
- **[Mention that you wanted to take this opportunity to introduce yourself and offer your assistance to the state in their efforts to enhance election infrastructure security]**
- **[Confirm that you are speaking with the correct election official for coordination with DHS, as not all states use the same structure]**
- **[Leverage this meeting to hear your state POC's hopes/concerns/suggestions for the way forward on this issue.]**

Talking Points

Designation as Critical Infrastructure Subsector

- As you may know, the Secretary of Homeland Security designated Election Infrastructure as a critical infrastructure subsector of Government Facilities in January 2017. DHS has no plans to change the designation under the current Administration.
- Typically, under the critical infrastructure subsector designation, partners organize for their collective good and receive prioritized assistance from the federal government for their efforts to manage risks to the sector or subsector.
- I want to stress that this assistance from the federal government is voluntary.
- The National Infrastructure Protection Plan provides general information on the benefits of this partnership and outlines how government and private sector partners work together to manage risks and achieve security.

Analytical Products under Development for the Subsector

- Our Office of Cyber and Infrastructure Analysis (OCIA) is working with Election Infrastructure stakeholders to develop a definition of the subsector that incorporates the appropriate elements that encompass the subsector, to include election officials, associations, and manufacturers of equipment, voter databases, systems, networks, and assets for voting, recording, and tabulating results.
- In addition to the near-term effort, OCIA is preparing to conduct risk assessments for states with 2017 major elections and a comprehensive subsector risk assessment by the end of 2017.

Information Sharing Processes and Available Resources

- Perhaps one of our greatest areas of mutual interest is in sharing information.
- We are offering assistance to state and local election officials to enhance efforts they have already been taking to secure their elections, informed by all relevant intelligence reporting.

- We can help increase awareness of potential vulnerabilities and promote security practices.
- In addition, and complementary to, assistance offered through the National Cybersecurity and Communications Integration Center (NCCIC), we can also provide physical assessments. Again, such assistance is voluntary and does not entail regulation.
- The Department has provided a range of cyber support to partners and continues to do so. One example is cyber hygiene scans on Internet-facing systems. These scans 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. For access to the full range of cyber resources DHS brings to bear, please contact SLTTCyber@hq.dhs.gov.
- The Department can also provide assistance in support of risk and vulnerability assessments. These assessments can be physical or cyber focused. To date, the cyber assessments have been the focus. They 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.
- Onsite assistance is a fairly limited resource, but elections infrastructure are a high priority for our department and we will work with our state and local partners to try and honor every request for assistance.
- The Department will continue to share relevant information on cyber and physical incidents through multiple means. For cyber activity, 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. All states are members of the MS-ISAC.

- It has representatives co-located with the NCCIC to enable regular collaboration and access to information and services for State Chief Information Officers (CIOs) and fusion centers.
- Election officials can connect with their State CIO or fusion center to benefit from this partnership and rapidly receive information they can use to protect their systems.
- We also 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 critical infrastructure systems. This technical information will also be shared with other states, without identifying the source, to assist their ability to defend their own systems from similar malicious activity.
- Additional service offerings are provided through our field offices.
 - DHS has personnel available in the field, Cybersecurity Advisors (CSAs) and Protective Security Advisors (PSAs), 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.
- The Department also offers a number of physical security tools, training, and resources. This information can be found online at www.dhs.gov/hometown-security. These products help 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.

Election Infrastructure Subsector - Frequently Asked Questions

Critical Infrastructure Designation Benefits

Q: What benefits to states does the subsector designation offer?

A: Participation in the subsector is voluntary and offers a number of potential benefits to states and localities, as well as to private sector members. It enables DHS to prioritize cybersecurity assistance to election officials, for those who request it. It 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. And the designation makes it easier for the federal government to have full and frank discussions with key stakeholders regarding sensitive vulnerability information by protecting that information from disclosure.

The National Infrastructure Protection Plan (NIPP) outlines how government and private sector participants in the critical infrastructure community work together to manage risks and achieve security and resilience outcomes. The partnership model set forth in the NIPP provides a well-tested supporting structure to bring together all stakeholders on the issue of election security and other critical infrastructure issues.

The council structure serves as a mechanism to facilitate more timely and coordinated information and threat sharing between DHS and partners in each sector, including through classified information forums.

Establishing the subsector will offer a more reliable and consistent approach to collaborative efforts on election security by formalizing processes and structures that have been initiated since DHS began working with state partners on election security in the run up to the 2016 elections.

The designation of election infrastructure as critical infrastructure does not change the primary role of state and local governments have in administering and running elections. It also does not create any new regulations.

Q: Will any additional funding be made available to states as part of the subsector designation?

A: The designation itself does not include a mechanism for providing funding to subsector members. However, state and local government officials will be able to utilize prioritized services from the Department of Homeland Security, including cybersecurity scans and technical assistance, which are offered on a voluntary basis free of charge.

Critical Infrastructure Designation Process

Q. How were the states and other parts of the election infrastructure engaged before DHS made this designation?

A. Previous DHS Secretary Jeh Johnson and DHS leadership engaged the Secretaries of State, state election officials, local election officials, and state security officials on calls in August and October 2016, and January 2017, and considered and respected the letters addressed to DHS on the critical infrastructure topic. Due to the importance of the nation's election infrastructure and the level of threats against it, former Secretary Johnson made the designation.

Since then, the Department has highlighted the vital importance of election infrastructure and reiterated his commitment to the critical infrastructure designation.

Q. How can we be certain that participation will remain voluntary?

A. The overall collaboration framework supporting the critical infrastructure sector construct is based on voluntary participation, as set forth in the National Infrastructure Protection Plan.

Q. Does PPD 21 designate DHS the lead for election security, or are the states still the lead?

A. Presidential Policy Directive 21 (PPD 21) does not designate DHS the lead for election security. That responsibility resides with state and local governments.

The critical infrastructure designation and establishment of DHS as the Sector-Specific Agency charges DHS with the responsibility to serve as the Federal interface for coordination of activities related to critical infrastructure security and resilience.

PPD 21 directs the Secretary of Homeland Security to evaluate the need for, and approve changes to, critical infrastructure sectors, in consultation with the Assistant to the President for Homeland Security and Counterterrorism before changing a critical infrastructure sector or a designated Sector-Specific Agency for that sector.

Q. Will states be required to conform to new federal standards?

A. No. The process of establishing and running a critical infrastructure sector or subsector does not entail creating or implementing federal standards. Partners within each critical infrastructure sector or subsector jointly collaborate – on a voluntary basis – to develop their own coordination processes and information sharing protocols, although on request DHS can offer templates and good practices based on what has worked for other critical infrastructure sectors.

Q. What if some states do not participate in the voluntary structure?

A. The sector structure offers effective coordination and threat information sharing processes that can improve the timeliness and depth of information shared between the federal government and sector partners. States that do not participate might not be able to benefit from the robust coordination processes put in place through the council structure.

Q. Does this mean DHS will not share information with states that do not participate in the voluntary structure?

A. DHS will continue to share timely, actionable threat information and offer cybersecurity assistance regardless of whether a state participates. However, states that choose not to participate may not be able to take advantage of some of the benefits the designation has to offer, such as the protections of critical infrastructure information from disclosure or the ability to receive classified information from intelligence agencies.

Q. What is the role of the Critical Infrastructure Protection Advisory Council (CIPAC) in the sector structure?

A. The sector councils may meet within the protections of the Critical Infrastructure Protection Advisory Council (CIPAC) structure, which allows members to meet with the federal government to discuss key issues impacting the sector and provide consensus advice to the federal government on these issues. The CIPAC protections are meant to promote the security and resilience of critical infrastructure, and should in no way impact transparency in the electoral process itself.

Threats and Clearance Process**Q. How can Secretaries of State get authorized to receive classified threat information from our intelligence agencies?**

A. The DHS Office of Intelligence and Analysis (I&A) manages the security clearance program supporting state and local government officials.

Security clearance request for Secretaries of State and Election Officials would be submitted through the I&A process, which requires nominations to be processed through the State Homeland Security Advisor's Office for submission to DHS, in order to continue to leverage existing and proven procedures.

In addition to facilitating processing of security clearances, DHS is also committed to rapidly providing critical infrastructure partners with actionable, unclassified threat information as soon as it is available to support decision-making and enhance situational awareness across the subsector.

Q. How soon can state officials expect to receive their clearances?

A. DHS will coordinate with the appropriate Election Infrastructure Subsector stakeholders to identify those individuals who will require clearances. We will leverage established nomination processes for our State and Local partners to ensure effective and efficient processing of clearance requests for Secretaries of State and/or State's Chief Elections Officials, as appropriate.

Q. What are the threats we are facing?

A. Multiple elements of election infrastructure are potentially vulnerable to cyber intrusions and cyber actors that may have an interest in targeting it. The risk to U.S. computer-enabled election systems varies from county to county, between types of devices used, and among processes used by polling stations.

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 and information technology resources available only to a nation-state. However, the level of effort and scale required to change the outcome of a national election would make it nearly impossible to avoid detection. As with other developments in the overall cyber environment, the spread of disruptive technologies has the ability to disrupt electoral processes. For example, targeted intrusions against individual voter registration databases remain possible. With illicit access, manipulation of voter registration data or disruptions to their availability may impact a voter's ability to vote on Election Day, or create confusion and uncertainty.

Most but not all jurisdictions still rely on paper voter rolls or electronic poll books that are not connected in real-time to voter registration databases, which limited the possible impacts in 2016. We are working with industry and stakeholders to enhance election infrastructure security and resilience.

Q. Can you tell me more about the cyber targeting of 21 states in the run-up to the 2016 election?

A. Regarding the 2016 election, the Department of Homeland Security is aware of suspicious activity targeting Internet-connected election-related networks across the country in at least 21 states targeted by Russian government actors.

DHS or its partners engaged with these affected entities. Information shared between DHS and critical infrastructure entities is protected and may be proprietary. This is necessary to ensure continued robust participation in our voluntary information sharing programs.

Although we've refined our understanding of individual targeted networks, supported by classified reporting, the scale and scope noted in that October 2016 report still generally characterizes our observations:

- A small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.

Governance Structure

Q. How many councils should there be?

A: Critical infrastructure sectors and subsectors establish a governance structure based on coordinating councils.

- The Sector Coordinating Council (SCC) serves as industry's principal entity for coordinating with the government on critical infrastructure security activities and issues. This council serves as the principal sector policy coordination and planning entities and enable owners and operators to interact on sector-specific strategies, policies, activities, and issues. In general, the SCC is self-organized, self-run, and self-governed, with a leadership structure directly designated by the sector membership. SCC membership will vary from sector to sector, reflecting the unique composition of each sector; however, membership should be representative of a broad base of owners, operators, industry associations, and other non-government entities—both large and small—within a sector.
- The Government Coordinating Council (GCC) serves as the government counterpart for each SCC to enable interagency and cross-jurisdictional coordination. They typically include representatives from across various levels of government (Federal, State, local, or tribal), as appropriate to the operating landscape of each individual sector. The GCC is chaired by a representative from the designated Sector-Specific Agency (SSA) with responsibility for ensuring appropriate representation on the GCC and providing cross-sector coordination with State, local, and tribal governments.

The common purpose of these councils is to enable Federal, State, Local, Tribal, and Territorial government organizations and private sector entities to collaborate through voluntary partnership mechanisms with the joint objective of enhancing critical infrastructure security and resilience.

While there is flexibility in how to set up sector councils, DHS can offer recommendations based on what works in other sectors. We recommend one GCC and one SCC to meet the primary purpose of multi-jurisdictional government coordination and public-private sector collaboration.

Q: Who should be on the Government Coordinating Council?

A: The GCC typically includes representatives from across various levels of government (Federal, State, local, or tribal), as appropriate to the operating landscape of the specific critical infrastructure sector or subsector.

Q: Who has input and final say on the GCC charter?

A: The designated SSA will convene the groups of interested critical infrastructure stakeholders and they will collectively develop the charter. Charters are agreed upon collaboratively and signed off on by representatives of all participating members.

Q: Does the charter get established before the council is formed?

A: No. The SSA will convene the groups of interested critical infrastructure stakeholders and they will collectively develop the GCC charter, to tailor it to their perceived needs for coordination and collaboration.

Q: Should there be one council or separate councils for state and local?

A: Critical infrastructure sectors have a single GCC chaired or co-chaired by the designated SSA to meet the primary purpose of government coordination and collaboration. We do not recommend a multi-council solution based on different levels of government as this may not be conducive to effective collaboration and coordination. Within the GCC council structure, participating critical infrastructure partners may, at their discretion, form special sub-groups (working groups, task forces, etc.) involving specific members to tackle key issues or concerns.

Q: Who should be on the Sector Coordinating Council?

A: The SCC is the private sector counterpart to the GCC and it generally includes owners, operators, industry associations, and other non-government entities. This can encompass a range of entities. In the case of election infrastructure, for instance, it might include equipment manufacturers, software companies, academia and research centers, think tanks, trade associations and other non-government organizations that have a role in election infrastructure.

Q: Who has input and final say on the SCC charter?

A: The SCC is self-organized, self-run, and self-governed, with a leadership structure directly designated by its membership. Charters are agreed upon collaboratively and signed off on by representatives of all participating members.

Q: Does the charter get established before the council is formed?

A: No. The critical infrastructure stakeholders interested in participating in the SCC will collectively develop the corresponding charter.

Q: Does DHS have charter templates to share?

A: Yes. We can offer a full range of templates that have been used by other critical infrastructure sectors and subsectors to establish their governance structures. Election Infrastructure Subsector stakeholders can choose to use these templates, revise them, or create new ones.

Q: Does DHS have a timeline with milestones?

A: At this time, we do not have specific subsector formation timelines. Ongoing subsector formation discussions and engagements with State and local election officials are providing the required forums for stakeholders to better understand the subsector formation process. This period allows time for communication and coordination amongst themselves and with other government entities as we collectively begin to determine an optimum governance framework, council makeup, goals and objectives of formation, and potential services available.

Q: What role do advocacy groups and interested third party organizations play? Should we plan to form an informal advisory group with these folks?

A: Depending on whether they are government or private sector organizations, they can be added to the respective GCC or SCC council structure as Subject Matter Experts (SMEs).

Q: What role, if any, does the Critical Infrastructure Partnership Advisory Council (CIPAC) play?

A: The Election Infrastructure Subsector is part of the CIPAC structure. The sector councils may meet within the protections of the Critical Infrastructure Protection Advisory Council (CIPAC) structure, which allows members to meet with the federal government to discuss key issues impacting the sector and provide consensus advice to the federal government on these issues.

The CIPAC protections are meant to promote the security and resilience of critical infrastructure, and should in no way impact transparency in the electoral process itself.

Q: The Election Lab at MIT (i.e. Charles Stewart III) has offered to help state and local officials create an ISAC for information dissemination. Does this sound like a reasonable idea?

A: While that decision should be jointly made by the subsector partners participating in the subsector council structure, they may wish to start with an established Information Sharing and

NPPD Field-Based Engagement with State Chief Election Officials

Background

- Federal, state and local officials, and the private sector all have a role to play in protecting the election subsector from the variety of threats to our critical infrastructure.
- The designation of election infrastructure as critical infrastructure does not change the primary role state and local governments have in administering and running elections, it does not create new regulations, and it does not give DHS new powers to intervene.
- Many state and local election organizations have been doing excellent work already to secure the election systems, and we believe that we can bring additional value to this effort, on an as-requested basis.

Discussion Guide

- **[Introduce yourself and mention that you are following up on conversations that have been initiated between state election officials and DHS headquarters.]**
- **[Explain your role as the Regional Director and acknowledge that the election official may also have heard from a cyber advisor, but you are part of the same team under the National Protection and Programs Directorate.]**
- **[Mention that you wanted to take this opportunity to introduce yourself and offer your assistance to the state in their efforts to enhance election infrastructure security]**
- **[Confirm that you are speaking with the correct election official for coordination with DHS, as not all states use the same structure]**
- **[Leverage this meeting to hear your state POC's hopes/concerns/suggestions for the way forward on this issue.]**

NPPD FIELD-BASED ENGAGEMENT INFORMATION ON ELECTION SECURITY

BACKGROUND

- Federal, state and local officials, and the private sector all have a role to play in protecting the election subsector from the variety of threats to our critical infrastructure.
- The designation of election infrastructure as critical infrastructure does not change the primary role state and local governments have in administering and running elections, it does not create new regulations, and it does not give DHS new powers to intervene.
- Many state and local election organizations have been doing excellent work already to secure the election systems through the National Association of Secretaries of State (NASS) and its Election Security Task Force. NASS published Areas of Shared Interest between states in the 21 July 2017 NASS *Issue Briefing* and DHS believes that it can bring additional value to securing future elections, on an as-requested basis.
- Deputy Undersecretary Kolasky tasked IP Regional Directors (RD) with contacting State Chief Election Officials (CEO) to ensure they are familiar with the capabilities and resources offered by NPPD, and that the RDs gain understanding of the specific election-related needs of the States within their region.

AREAS OF SHARED INTEREST & DHS ASSISTANCE OFFERING

1) Establishing clear and effective structures for threat and intelligence information-sharing, victim notification processes and cyber incident response, including:

NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Obtaining federal government security clearances for Secretaries of State/Chief State Election Officials in order to access timely threat information to protect election systems. 	<ul style="list-style-type: none"> • DHS Office of Intelligence and Analysis (I&A) has offered assistance with security clearances. Security clearance requests requires nominations to be processed through the State Homeland Security Advisor’s Office for submission to DHS I&A, in order to continue to leverage existing and proven procedures. • In addition to facilitating processing of security clearances, DHS is also committed to rapidly providing critical infrastructure partners with actionable, unclassified threat information as soon as it is available.
NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Improving government processes for notifications regarding system attacks and breaches. 	<ul style="list-style-type: none"> • DHS Cybersecurity Advisors (CSA) and Protective Security Advisors (PSA) can

NPPD FIELD-BASED ENGAGEMENT INFORMATION ON ELECTION SECURITY

	<p>assess current processes and provide advice for improvements in this area.</p>
<ul style="list-style-type: none"> • Establishing a Critical Infrastructure State Government Coordinating Council to interface with federal agencies regarding election security issues. 	<ul style="list-style-type: none"> • The Election Infrastructure Subsector Government Coordinating Council will enable interagency and cross-jurisdictional coordination. • DHS Office of Cyber and Infrastructure Analysis (OCIA) is working with Election infrastructure stakeholders to develop a definition of the subsector that incorporates the appropriate elements that encompass the subsector, to include election officials, associations, and manufacturers of equipment, voter databases, systems, networks, and assets for voting, recording, and tabulating results.
<ul style="list-style-type: none"> • Leveraging MS-ISAC/State Fusion Centers for continuous monitoring, threat detection and incident awareness/response. 	<ul style="list-style-type: none"> • DHS CSAs, PSAs, and Intelligence Officers are also integrated with the MS-ISAC and State Fusion Centers in order to share actionable intelligence with stakeholders.
<ul style="list-style-type: none"> • Developing state-specific frameworks for cyber incident response, in the event of a major attack. 	<ul style="list-style-type: none"> • DHS CSAs and PSAs can assess current processes and provide advice for improvements in this area.

NPPD FIELD-BASED ENGAGEMENT INFORMATION ON ELECTION SECURITY

2) Identifying threat mitigation practices and state policy trends for consideration, including:

NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Under a risk-based model like the NIST Cybersecurity Framework, some states are trying to develop more of an enterprise mentality to improving cybersecurity coordination and response. 	<ul style="list-style-type: none"> • DHS offers coordination for cyber-related incident response through its National Cybersecurity and Communications Integration Center (NCCIC). • DHS and State Homeland Security organizations have the ability to invite stakeholders to collaborate and plan for elections through use of the IP Gateway tool and the Homeland Security Information Network (HSIN).
NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Reviewing/updating policies for back-up paper ballots and equipment, paper printouts/records for polling place use, post-election audits, back-up voter lists (paper and electronic) and voter data security. 	<ul style="list-style-type: none"> • DHS I&A and IP can help inform policy through the identification of threats to, and vulnerabilities in, the election process. • DHS Office of Cyber and Infrastructure Analysis (OCIA) can evaluate the consequences of a potential disruption from physical or cyber threats and incidents. The results of this analysis informs decisions about infrastructure security and resilience, as well as response and recovery efforts.

NPPD FIELD-BASED ENGAGEMENT INFORMATION ON ELECTION SECURITY

3) Conducting risk assessments and implementing continuous vulnerability assessments, including:

NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Regularly monitoring election system threats and vulnerabilities to defend any related cyber networks against attacks, including phishing scams, malware, denial-of-service attacks and other common practices employed by malicious actors. 	<ul style="list-style-type: none"> • DHS will continue to share relevant information on cyber and physical incidents through multiple means. For cyber activity, the NCCIC and CSAs work with the MS-ISAC to provide threat and vulnerability information to state and local officials.
<ul style="list-style-type: none"> • Working with in-house IT advisors, private security partners, state CIOs/CISOs, Homeland Security Advisors, the Department of Homeland Security and others to ensure that state election systems are secured with technologies and standard operating practices that can successfully diagnose potential cyber threats, track cyberattacks, provide mitigation options and enhance the resilience of state systems. 	<ul style="list-style-type: none"> • DHS CSAs and PSAs can provide actionable information and connect election officials to a range of tools and resources available to improve the cybersecurity preparedness of election systems to include the physical site security of voting machine storage and other significant assets. • These Advisors are also available to assist with planning and incident management assistance for both cyber and physical incidents.
<ul style="list-style-type: none"> • Documenting and reviewing all security procedures/systems, including pre- and post-election protocols and testing procedures, physical security and chain of custody policies and response to reported hardware/software issues. 	<ul style="list-style-type: none"> • DHS can help identify Federal, state and local partners to assist in this effort.

NPPD FIELD-BASED ENGAGEMENT INFORMATION ON ELECTION SECURITY

4) Ensuring that election offices have sufficient equipment, technical support and resources to maintain a sound security posture for their computer-based systems, including:

NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Consulting with key stakeholders (i.e. Members of Congress, Governor, state legislators, state CIO/CISO) regarding current levels of investment in state and local election infrastructure. Request cybersecurity briefing from Governor/State CIO or CISO. 	<ul style="list-style-type: none"> • DHS CSAs can provide technical assistance regarding cybersecurity aspects for investments in election infrastructure. DHS can support cybersecurity briefings with relevant cyber and physical information through multiple means.
<ul style="list-style-type: none"> • Replacing aging voting equipment that is nearing end of life, no longer meets state testing and certification requirements, or will soon fail to meet such requirements due to lack of technical support/replacement parts. 	<ul style="list-style-type: none"> • DHS CSAs can provide technical assistance regarding cybersecurity aspects for investments in election infrastructure.
NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Bringing laws and policies guiding election administration into compliance with existing legal exemptions for critical infrastructure information-sharing under federal law. 	<ul style="list-style-type: none"> • The Election Infrastructure Subsector Government Coordinating Council can serve as a collaborative platform to establish leading practices for information-sharing.

5) Fostering a culture of risk awareness with strong cyber hygiene practices, including:

NASS Task	DHS Assistance Offering
<ul style="list-style-type: none"> • Training or guidance on cyber hygiene protocols for elections officials, along with establishing clear communication protocols between state-local officials. 	<ul style="list-style-type: none"> • DHS CSAs and PSAs can assess current processes and provide advice for establishing clear communications protocols.
<ul style="list-style-type: none"> • Providing guidance on procedures for reporting election issues and security-related incidents (i.e. state hotlines, poll worker guidance, state task force, DHS/FBI coordination, state fusion center with law enforcement). 	<ul style="list-style-type: none"> • DHS CSAs and PSAs can provide guidance for reporting security-related incidents between state and federal agencies.

Can you tell me more about the cyber targeting of 21 states in the run-up to the 2016 election?

- A. Regarding the 2016 election, the Department of Homeland Security is aware of suspicious activity targeting Internet-connected election-related networks across the country in at least 21 states targeted by Russian government actors.

DHS or its partners engaged with these affected entities. Information shared between DHS and critical infrastructure entities is protected and may be proprietary. This is necessary to ensure continued robust participation in our voluntary information sharing programs.

Although we've refined our understanding of individual targeted networks, supported by classified reporting, the scale and scope noted in that October 2016 report still generally characterizes our observations:

- A small number of networks were successfully compromised, there were a larger number of states where attempts to compromise networks were unsuccessful, and there were an even greater number of states where only preparatory activity like scanning was observed.



Homeland
Security

August 3, 2017

ACTION MEMORANDUM

MEMORANDUM FOR DISTRIBUTION

FROM: Bob Kolasky
(Acting) Deputy Under Secretary *BK*

THROUGH: Scott Breor, Director, Protective Security Coordination Division

TO: IP Regional Directors

CC: Jeanette Manfra, Assistant Secretary for Cybersecurity and Communications

SUBJECT: NPPD Field-based Engagement with State Chief Election Officials

Purpose: To promulgate guidance for Office of Infrastructure Protection (IP) Regional Directors to engage with their respective state Chief Election Official, normally the Secretary of State, in order to ensure awareness of the NPPD capabilities and to better understand the Chief Election Official's (CEO) election infrastructure related needs.

Background: In January 2017, the Department designated the Nation's Election Infrastructure as a subsector of the Government Facilities Sector. Secretary Kelly affirmed this subsector designation. The National Protection and Programs Directorate (NPPD) has been designated as the Election Infrastructure Sector Specific Agency (SSA). The SSA lead role has been delegated to IP, with the Sector Outreach and Programs Division (SOPD) executing the corresponding SSA management responsibilities.

Action: NPPD is energizing all available resources to support the development of this important subsector and its key stakeholders. An NPPD enterprise-wide approach in this emergent effort is essential for sustained progress. Your direct engagement is needed to ensure broad understanding and gain support for this emerging subsector development effort.

As such, I am directing that each IP Regional Director make themselves available to meet with State's Chief Election Officials to ensure the CEO is familiar with the capabilities and resources of the IP Regional Team and that you, as Regional Director, better understand the specific election-related needs of the States within your region. Please do so in coordination with locally-based

Cyber Security Advisors in your region and any Protective Security Advisors who will have ongoing responsibility for working with Election officials.

In order to help prepare you for these meetings, the Election Infrastructure SSA team will send you a set of talking points, relevant NPPD assistance, and a listing of State Chief Election Officials by Friday, August 4 2017. Once talking points are received, these engagements should take place over the next 60 days with after-action reports, compiled via PSCD, sent back to me with copy to Juan Figueroa, who leads the Election Infrastructure SSA team.

Timeliness: Please ensure engagement completion across all ten regions and submittal of the corresponding after-action reports by Tuesday, October 3, 2017.

Distribution:

- A. IP Regional Directors (Regions I-X)
- B. David Wulf, Deputy Assistant Secretary, Office of Infrastructure Protection (Acting)
- C. Steven Nider, Chief of Staff (Acting)
- D. Linda Solheim, Director, Sector Outreach and Programs Division
- E. Danny Toler, Deputy Assistant Secretary, Office of Cybersecurity and Communications
- F. Brad Tenney, Acting Director, Stakeholder Engagement and Cyber Infrastructure Resilience
- G. Brandon Wales, Director Office of Cyber and Infrastructure Analysis

Arizona

State Election and Cybersecurity Officials



MICHELE REAGAN **SECRETARY OF STATE, ARIZONA** **BIO**

In a state full of success stories, Secretary of State Michele Reagan has risen to Arizona's second highest elective office. Through a combination of hard work, commitment to public service and the pioneer spirit; she exemplifies what it means to be an Arizonan.

Moving from the south suburbs of Chicago in 1991, Secretary Reagan adopted Arizona as her second home and opened FASTSIGNS in Phoenix, learning quickly about the issues that face the state's small businesses each day. Her steadfast advocacy for small business, community involvement, fiscal conservatism and a desire to do more became the catalyst to run for public office.

Secretary Reagan's illustrious career in public service has spanned more than a decade in both houses of the legislature. Recognized as the tireless champion of small businesses, Ms. Reagan was named Chair of the Commerce Committee in the House, and later, Chair of the Economic Development and Jobs Creation Committee in the Senate.

During her candidacies for office, Secretary Reagan developed a passion for fair, accurate and efficient elections. This passion contributed to the formation of the first Senate Elections Committee, of which she was Chair. She was encouraged by community advocates, state and local leaders, and the last four Secretaries of State to run for the state's second highest office. Ms. Reagan was elected to serve as Arizona's 20th Secretary of State 2014

State Election and Cybersecurity Officials

Secretary Reagan's distinguished career has earned her numerous awards and accolades including: Small Business Guardian from the National Federation of Independent Business, the Eye of the Eagle Award from the Arizona Small Business Association and one of the 50 most Influential Women in Arizona by AZBusiness Magazine in 2013.

Secretary Reagan proudly serves on the Lieutenant Governors Association's Board representing the Western states. She also serves on the Advisory Boards of Childhelp USA and Worldly Kids.

Secretary Reagan is a graduate of Illinois State University and was named by the Aspen Institute to its prestigious Rodel Fellowship, a program designed to bring together elected officials who have demonstrated an outstanding ability to work responsibly across partisan divisions and bring greater civility to public discourse.

Mrs. Reagan is married, has a stepdaughter, three dog children, and a desert tortoise named Casey.

State Election and Cybersecurity Officials



GILBERT M. ORRANTIA
DIRECTOR, ARIZONA DEPARTMENT OF HOMELAND SECURITY

Gilbert Orrantia became the Director of the Arizona Department of Homeland Security in June, 2009. Prior to heading Arizona's Homeland Security efforts at the State, he served in the FBI for 26 years.

Director Orrantia brings a national and global perspective on counterterrorism that is gained from vast counterterrorism experience including the supervision of an FBI counterterrorism squad in Phoenix and serving eight years as a Supervisory Special Agent. For four years he helped lead the FBI's Joint Terrorism Task Force in Phoenix, Arizona located at Arizona's fusion center, known as the Arizona Counter Terrorism Information Center (ACTIC).

Recognized as an expert in investigations of terrorism, drugs and violent crimes, Mr. Orrantia's successful FBI law enforcement career is reflected in the numerous awards and commendations he received. Among them are two of the FBI's highest commendations: the Medal of Valor and the FBI Star. These awards were made to Mr. Orrantia for his role in the deadliest firefight in FBI history;- a gun battle known as the "Miami Shootout" in which two fellow FBI agents were killed. Director Orrantia has lectured to members of the FBI Academy at Quantico, Virginia on officer safety and survival and continues to share his expertise in surviving a deadly encounter with numerous law enforcement agencies.

State Election and Cybersecurity Officials

Director Orrantia currently serves on the executive committee of the National Governors Association Homeland Security Advisors Council and also serves as the Co-Chair of the Governor's Arizona Human Trafficking Council.

Director Orrantia, a native Arizonan who is fluent in Spanish, was raised in Mesa, Arizona. He is a graduate of Arizona State University with a Bachelor of Arts degree in Education.

State Election and Cybersecurity Officials



DOUG DUCEY GOVERNOR, ARIZONA

BIO

Governor Doug Ducey is the 23rd governor of the state of Arizona. He was elected on November 4, 2014 and sworn into office on January 5, 2015 – inheriting a \$1 billion budget deficit.

With a mission to make Arizona the best state in the country to live, work, do business and get an education, Governor Ducey and state leaders got to work. Today, Arizona’s budget is balanced. Business is thriving. And public schools continue to improve.

The governor remains committed to what he has identified as his top priorities: growing the economy, creating and supporting 21st-century jobs, promoting educational excellence, protecting our communities and restoring fiscal responsibility – all without raising taxes on hardworking Arizonans. State Election and Cybersecurity Officials

A strong Arizona is an Arizona that ensures “Opportunity For All.” Governor Ducey has pledged to work every day to make that vision a reality.

State Election and Cybersecurity Officials

Governor Doug Ducey was born in Toledo, Ohio. He moved to Arizona to attend Arizona State University's business school, where he earned his bachelor of science in finance in 1986. He is the former CEO of Cold Stone Creamery. Governor Ducey and his wife, Angela, live in Paradise Valley with their three sons, Jack, Joe and Sam.

Election Infrastructure Information

Counties: 15

Voter Registration/Qualifications: To vote in Arizona, one must be a citizen of the United States and a resident of an Arizona county. A voter must be 18 years or older on or before Election Day. To be eligible to vote in an election one must register at least 29 days prior to the election. Voting rights for convicted criminals vary substantially from state to state. In the vast majority of states, convicted criminals cannot vote while they are incarcerated, but may regain the right to vote upon release from prison or at some point thereafter. Arizona is one of eight states in which criminals with certain convictions never regain the right to vote. A citizen can register online, in person at the county recorder's office or by mail. Citizens must provide proof of citizenship to register to vote. Acceptable forms of documentation include birth certificates, passports and U.S. naturalization documents.

Voter Equipment used to cast ballots: Arizona uses paper and Direct Recording Electronic (DRE) systems for its elections. The state does require a voter-verified paper audit trail (VVPAT) when conducting elections. According to the National Academy of Sciences, a voter-verified paper audit trail "consists of physical paper records of voter ballots as voters have cast them on an electronic voting system. In the event that an election recount or audit is called for, the VVPAT provides a supporting record."

Arizona Revised Statutes Vote Counting, Title 16, Chapter 6, 2014 (Security):

16-602. Removal of ballots from ballot boxes; disposition of ballots folded together or excessive ballots; designated margin; hand counts; vote count verification committee.

A. For any primary, special or general election in which the votes are cast on an electronic voting machine or tabulator, the election judge shall compare the number of votes cast as indicated on the machine or tabulator with the number of votes cast as indicated on the poll list and the number of provisional ballots cast and that information shall be noted in a written report prepared and submitted to the officer in charge of elections along with other tally reports.

B. For each countywide primary, special, general and presidential preference election, the county officer in charge of the election shall conduct a hand count at one or more secure facilities. The hand count shall be conducted as prescribed by this section and in accordance with hand count procedures established by the secretary of state in the official instructions and procedures manual adopted pursuant to section 16-452. The hand count is not subject to the live video requirements of section 16-621, subsection C, but the party representatives who are observing the hand count may bring their own video cameras in order to record the hand count. The recording shall not interfere with the conduct of the hand count and the officer in charge of the election may prohibit from recording or remove from the facility persons who are taking actions to disrupt the count. The sole act of recording the hand count does not constitute sufficient grounds for the officer in charge of the election to prohibit observers from recording or to remove them from the facility. The hand count shall be conducted in the following order:

1. At least two per cent of the precincts in that county, or two precincts, whichever is greater, shall be selected at random from a pool consisting of every precinct in that county. The county political party chairman for each political party that is entitled to continued representation on the state ballot or the

Election Infrastructure Information

chairman's designee shall conduct the selection of the precincts to be hand counted. The precincts shall be selected by lot without the use of a computer, and the order of selection by the county political party chairmen shall also be by lot. The selection of the precincts shall not begin until all ballots voted in the precinct polling places have been delivered to the central counting center. The unofficial vote totals from all precincts shall be made public before selecting the precincts to be hand counted. Only the ballots cast in the polling places and ballots from direct recording electronic machines shall be included in the hand counts conducted pursuant to this section. Provisional ballots, conditional provisional ballots and write-in votes shall not be included in the hand counts and the early ballots shall be grouped separately by the officer in charge of elections for purposes of a separate manual audit pursuant to subsection F of this section.

2. The races to be counted on the ballots from the precincts that were selected pursuant to paragraph 1 of this subsection for each primary, special and general election shall include up to five contested races. After the county recorder or other officer in charge of elections separates the primary ballots by political party, the races to be counted shall be determined by selecting by lot without the use of a computer from those ballots as follows:

(a) For a general election, one statewide ballot measure, unless there are no measures on the ballot.

(b) One contested statewide race for statewide office.

(c) One contested race for federal office, either United States senate or United States house of representatives. If the United States house of representatives race is selected, the names of the candidates may vary among the sampled precincts.

(d) One contested race for state legislative office, either state house of representatives or state senate. In either case, the names of the candidates may vary among the sampled precincts.

(e) If there are fewer than four contested races resulting from the selections made pursuant to subdivisions (a) through (d) and if there are additional contested federal, statewide or legislative races or ballot measures, additional contested races shall be selected by lot not using a computer until four races have been selected or until no additional contested federal, statewide or legislative races or ballot measures are available for selection.

(f) If there are no contested races as prescribed by this paragraph, a hand count shall not be conducted for that precinct for that election.

3. For the presidential preference election, select by lot two per cent of the polling places designated and used pursuant to section 16-248 and perform the hand count of those ballots.

4. For the purposes of this section, a write-in candidacy in a race does not constitute a contested race.

5. In elections in which there are candidates for president, the presidential race shall be added to the four categories of hand counted races.

Election Infrastructure Information

6. Each county chairman of a political party that is entitled to continued representation on the state ballot or the chairman's designee shall select by lot the individual races to be hand counted pursuant to this section.

7. The county chairman of each political party shall designate and provide the number of election board members as designated by the county officer in charge of elections who shall perform the hand count under the supervision of the county officer in charge of elections. For each precinct that is to be audited, the county chairmen shall designate at least two board workers who are registered members of any or no political party to assist with the audit. Any qualified elector from this state may be a board worker without regard to party designation. The county election officer shall provide for compensation for those board workers, not to include travel, meal or lodging expenses. If there are less than two persons for each audited precinct available to participate on behalf of each recognized political party, the recorder or officer in charge of elections, with the approval of at least two county party chairpersons in the county in which the shortfall occurs, shall substitute additional individual electors who are provided by any political party from anywhere in the state without regard to party designation to conduct the hand count. A county party chairman shall approve only those substitute electors who are provided by the county chairman's political party. The political parties shall provide to the recorder or officer in charge of elections in writing the names of those persons intending to participate in the hand count at the audited precincts not later than 5:00 p.m. on the Tuesday preceding the election. If the total number of board workers provided by all parties is less than four times the number of precincts to be audited, the recorder or officer in charge of elections shall notify the parties of the shortage by 9:00 a.m. on the Wednesday preceding the election. The hand count shall not proceed unless the political parties provide the recorder or officer in charge of elections, in writing, a sufficient number of persons by 5:00 p.m. on the Thursday preceding the election and a sufficient number of persons, pursuant to this paragraph, arrive to perform the hand count. The recorder or officer in charge of elections may prohibit persons from participating in the hand count if they are taking actions to disrupt the count or are unable to perform the duties as assigned. For the hand count to proceed, no more than seventy-five per cent of the persons performing the hand count shall be from the same political party.

8. If a political party is not represented by a designated chairperson within a county, the state chairperson for that political party, or a person designated by the state chairperson, may perform the actions required by the county chairperson as specified in this section.

C. If the randomly selected races result in a difference in any race that is less than the designated margin when compared to the electronic tabulation of those same ballots, the results of the electronic tabulation constitute the official count for that race. If the randomly selected races result in a difference in any race that is equal to or greater than the designated margin when compared to the electronic tabulation of those same ballots, a second hand count of those same ballots and races shall be performed. If the second hand count results in a difference in any race that is less than the designated margin when compared to the electronic tabulation for those same ballots, the electronic tabulation constitutes the official count for that race. If the second hand count results in a difference in any race that is equal to or greater than the designated margin when compared to the electronic tabulation for those same ballots, the hand count shall be expanded to include a total of twice the original number of randomly selected precincts. Those additional precincts shall be selected by lot without the use of a computer.

Election Infrastructure Information

D. In any expanded count of randomly selected precincts, if the randomly selected precinct hand counts result in a difference in any race that is equal to or greater than the designated margin when compared to the electronic tabulation of those same ballots, the final hand count shall be extended to include the entire jurisdiction for that race. If the jurisdictional boundary for that race would include any portion of more than one county, the final hand count shall not be extended into the precincts of that race that are outside of the county that is conducting the expanded hand count. If the expanded hand count results in a difference in that race that is less than the designated margin when compared to the electronic tabulation of those same ballots, the electronic tabulation constitutes the official count for that race.

E. If a final hand count is performed for an entire jurisdiction for a race, the final hand count shall be repeated for that race until a hand count for that race for the entire jurisdiction results in a count that is identical to one other hand count for that race for the entire jurisdiction and that hand count constitutes the official count for that race.

F. After the electronic tabulation of early ballots and at one or more times selected by the chairman of the political parties entitled to continued representation on the ballot or the chairman's designee, the chairmen or the chairmen's designees shall randomly select one or more batches of early ballots that have been tabulated to include at least one batch from each machine used for tabulating early ballots and those ballots shall be securely sequestered by the county recorder or officer in charge of elections along with their unofficial tally reports for a postelection manual audit. The chairmen or the chairmen's designees shall randomly select from those sequestered early ballots a number equal to one per cent of the total number of early ballots cast or five thousand early ballots, whichever is less. From those randomly selected early ballots, the county officer in charge of elections shall conduct a manual audit of the same races that are being hand counted pursuant to subsection B of this section. If the manual audit of the early ballots results in a difference in any race that is equal to or greater than the designated margin when compared to the electronically tabulated results for those same early ballots, the manual audit shall be repeated for those same early ballots. If the second manual audit results in a difference in that race that is equal to or greater than the designated margin when compared to the electronically tabulated results for those same early ballots, the manual audit shall be expanded only for that race to a number of additional early ballots equal to one per cent of the total early ballots cast or an additional five thousand ballots, whichever is less, to be randomly selected from the batch or batches of sequestered early ballots. If the expanded early ballot manual audit results in a difference for that race that is equal to or greater than the designated margin when compared to any of the earlier manual counts for that race, the manual counts shall be repeated for that race until a manual count results in a difference in that race that is less than the designated margin. If at any point in the manual audit of early ballots the difference between any manual count of early ballots is less than the designated margin when compared to the electronic tabulation of those ballots, the electronic tabulation shall be included in the canvass and no further manual audit of the early ballots shall be conducted.

G. During any hand count of early ballots, the county officer in charge of elections and election board workers shall attempt to determine the intent of the voter in casting the ballot.

H. Notwithstanding any other law, the county officer in charge of elections shall retain custody of the ballots for purposes of performing any required hand counts and the officer shall provide for security for those ballots.

Election Infrastructure Information

I. The hand counts prescribed by this section shall begin within twenty-four hours after the closing of the polls and shall be completed before the canvassing of the election for that county. The results of those hand counts shall be provided to the secretary of state, who shall make those results publicly available on the secretary of state's website.

J. For any county in which a hand count has been expanded to all precincts in the jurisdiction, the secretary of state shall make available the escrowed source code for that county to the superior court. The superior court shall appoint a special master to review the computer software. The special master shall have expertise in software engineering, shall not be affiliated with an election software vendor nor with a candidate, shall sign and be bound by a nondisclosure agreement regarding the source code itself and shall issue a public report to the court and to the secretary of state regarding the special master's findings on the reasons for the discrepancies. The secretary of state shall consider the reports for purposes of reviewing the certification of that equipment and software for use in this state.

K. The vote count verification committee is established in the office of the secretary of state and all of the following apply:

1. At least thirty days before the 2006 primary election, the secretary of state shall appoint seven persons to the committee, no more than three of whom are members of the same political party.
2. Members of the committee shall have expertise in any two or more of the areas of advanced mathematics, statistics, random selection methods, systems operations or voting systems.
3. A person is not eligible to be a committee member if that person has been affiliated with or received any income in the preceding five years from any person or entity that provides election equipment or services in this state.
4. The vote count verification committee shall meet and establish one or more designated margins to be used in reviewing the hand counting of votes as required pursuant to this section. The committee shall review and consider revising the designated margins every two years for use in the applicable elections. The committee shall provide the designated margins to the secretary of state at least ten days before the primary election and at least ten days before the general election, and the secretary of state shall make that information publicly available on the secretary of state's website.
5. Members of the vote count verification committee are not eligible to receive compensation but are eligible for reimbursement of expenses pursuant to title 38, chapter 4, article 2. The committee is a public body and its meetings are subject to title 38, chapter 3, article 3.1 and its reports and records are subject to title 39, chapter 1.

Voting Equipment Security

The security of all voting equipment shall be given the same level of attention that one would give to official ballots.

1. Voting equipment shall be physically secured at all times. No physical access shall be given to any person unless the election officer in charge of the equipment specifically grants that person access.

Election Infrastructure Information

2. Immediately prior to loading the election, the officer in charge of elections shall reload the authorized operating environment from a known good source on any machine that is capable of software updating the operating environment and where doing so does not require disassembly of equipment or impact the manufacturer's warranty. The known good source for the operating environment shall originate from the vendor and shall be protected according to the section entitled "Election Media Security." The operating environment may include the operating system and the election software. This only applies to machines on which votes are cast.
3. Immediately after loading the election, each voting device or container shall be sealed utilizing one or more uniquely identified tamper-resistant or tamper-evident seals.
 - Logs shall contain a record of the voting device, the electronic media contained within, and the seal(s) securing the device.
4. The custody of voting machines from their election loading location, to storage, through the election process, to their final post election disposition and return to storage shall be tracked and documented.
 - The chain of custody shall utilize two or more individuals to perform a check and verification check whenever a transfer of custody takes place.
5. Vendor-supplied passwords shall not be used for access to voting equipment.
6. Each jurisdiction shall implement a recovery plan that is to be followed should there be any indication of a security breach involving voting equipment. Any indication of a security breach shall be confirmed by more than one individual.
7. Each jurisdiction shall implement a training plan for election officials, staff, and temporary workers that address these security procedures.

Election Media Security

Election media is any electronic or magnetic storage media that holds any election-related information. This includes identification cards, memory devices, and equipment that directly reads from and writes to these devices. The security of these media must be given the same level of attention that one would give to official ballots.

1. Each media shall be permanently identified with a unique serial number or identifier.
2. An inventory of all electronic media shall be created and maintained.
3. The custody of electronic media from their storage location, through election coding, through the election process, to their final post election disposition and return to storage shall be tracked and documented.
 - a. The chain of custody shall utilize two or more individuals to perform a check and verification check whenever a transfer of custody takes place.
4. Electronic media shall be physically secured at all times. No physical access should be given to any person unless the election officer in charge of the media specifically grants that person access. Secured locations must be provided for:
 - a. storing the electronic media when not in use
 - b. coding an election
 - c. creating the election media
 - d. transferring and installing the election media into the voting device

Election Infrastructure Information

5. No election media shall be left unattended or in an unsecured location once it has been coded for an election.
 - a. Where applicable, coded election media shall be immediately loaded into the relevant voting device, sealed, logged, and made secure or must be placed in a secured and controlled environment and inventoried.
 - b. Media that are device independent (e.g., Personal Electronic Ballots [PEBs], voter card encoders) shall be stored in a secured, sealed container and must also be identified on a master log.
6. Each jurisdiction shall implement a recovery plan that is to be followed should there be any indication of a security breach involving election media. Any indication of a security breach shall be confirmed by more than one individual.
7. Each jurisdiction shall implement a training plan for election officials, staff, and temporary workers that address these security procedures.

A person who knowingly modifies the software, hardware or source code for voting equipment without receiving approval or certification pursuant to section [A.R.S § 16-442](#) is guilty of a class 5 felony.

Election Infrastructure Information

Voting Systems Certification Process:

Arizona Voting System Certification Process

General Provisions

- Pursuant to A.R.S. § 16-442(B) beginning in January 2006 voting machines and devices used in federal, state or county elections may only be certified and used in Arizona if they have been tested to the appropriate voting system standards and approved by a laboratory that is accredited by the federal Election Assistance Commission (EAC), pursuant to P.L. 107-252. In addition to federal certification, all components of an electronic voting system must meet all requirements of Arizona State law.
- A.R.S. § 16-446 details the specific requirements for electronic voting machines:
 - A. An electronic voting system consisting of a voting or marking device in combination with vote tabulating equipment shall provide facilities for voting for candidates at both primary and general elections.
 - B. An electronic voting system shall:
 1. Provide for voting in secrecy when used with voting booths.
 2. Permit each elector to vote at any election for any person for any office whether or not nominated as a candidate, to vote for as many persons for an office as he is entitled to vote for, to vote for or against any question upon which he is entitled to vote, and the vote tabulating equipment shall reject choices recorded on his ballot card or paper ballot if the number of choices exceeds the number which he is entitled to vote for the office or on the measure.
 3. Prevent the elector from voting for the same person more than once for the same office.
 4. Be suitably designed for the purpose used, of durable construction, and may be used safely, efficiently and accurately in the conduct of elections and counting ballots.
 5. Be provided with means for sealing the voting or marking device against any further voting after the close of the polls and the last voter has voted.
 6. When properly operated, record correctly and count accurately every vote cast.
 7. Provide a paper document or ballot that visually indicates the voter's selections.
- Additional Provisions for the specific Arizona-Wyoming Ballot Rotation and other general requirements for voting equipment are found in A.R.S. Title 16 Chapter 4.

Election Infrastructure Information

- Pursuant to A.R.S. § 16-442(A): The Secretary of State shall appoint a committee of three persons (Committee), no more than two of whom shall be of the same political party, to investigate and test the various types of vote recording or tabulating machines or devices which may be used in state and local elections. They shall submit their recommendations to the Secretary of State who shall make final adoption.
- When considering voting equipment for Arizona certification, the Committee will take into consideration recommendations received pursuant to A.R.S. § 16-442.01.
- All electronic voting systems certified by the state will exactly match the system tested and approved by the Voting System Test Laboratories (VSTL). The system's digital software signature may be used for verification.
- Pursuant to A.R.S. § 16-1004(B): A person who knowingly modifies the software, hardware or source code for voting equipment without receiving approval or certification pursuant to section 16-442 is guilty of a class 5 felony.

Election Information

Upcoming Elections

2017 Consolidated Election Dates

ELECTION DATE	VOTER REGISTRATION DEADLINE
August 29, 2017	July 31, 2017
November 07, 2017	October 9, 2017 ¹

NOTE: County, city and local jurisdictions are responsible for administering elections on the above dates where applicable.

All voter registration deadlines are pursuant to A.R.S. §§ 16-120 & 16-134.

1. This date may be subject to change in some counties in light of the Columbus Day holiday. Please contact your County Recorder for more information.

2018 Election Dates

ELECTION DATE	VOTER REGISTRATION DEADLINE
March 13, 2018	February 12, 2018
May 15, 2018	April 16, 2018
August 28, 2018	July 30, 2018
November 06, 2018	October 8, 2018 ¹

Note: All voter registration deadlines are pursuant to A.R.S. §§ 16-120 & 16-134.

1. This date may be subject to change in some counties in light of the Columbus Day holiday. Please contact your County Recorder for more information.

Open Source Media Coverage

[How states are handling Trump's voter information request](#)

By The Associated Press
Aug 9, 2017.

These are state-by-state responses to a request for detailed voter data from President Donald Trump's Presidential Advisory Commission on Election Integrity, which is investigating voter fraud. The information indicates whether a state is willing to comply with, is denying or is undecided on the request for data. Some of the states that are willing to comply have fees or other requirements of the commission. All states that have agreed to provide the information are withholding some details that the commission said it wanted only if it was considered public under state law. The commission sent one request in late June and another in July after a court said the data collection could move ahead.

ARIZONA

Undecided

After initially saying the state would provide some records, Secretary of State Michele Reagan, a Republican, did an about-face and said the state wouldn't provide extensive voter registration information to the Trump administration. But on July 27, a spokesman said Reagan was asking a special counsel to review the latest version of the request. When she nixed sharing anything, Reagan cited privacy concerns.

[Feds Warn States to Batten down Hatches Following Election System Attacks](#)

By David Jones
Sep 2, 2016 7:00 AM PT

The FBI has launched investigations into malicious cyberattacks on the electronic election infrastructures in Illinois and Arizona, and federal officials last month warned states to take steps to protect their systems as the presidential campaign heats up, according to reports that surfaced this week.

The attacks, dating back to June, led to the illegal download of information on more than 200,000 Illinois voters, leading to a 10-day shutdown of the state's voter registration system. Hackers also penetrated systems in Arizona but apparently failed to download specific voter information. A timeline issued by the Illinois Board of Elections confirmed that it contacted the Illinois Attorney General's office, was contacted by the FBI, and has been cooperating with the agency.

SQL Attack

The attack on the Illinois voter registration database began on June 23 and was discovered on July 12, according to the timeline. The voter registration database apparently was the victim of an SQL injection attack, resulting from repeatedly entering an authorized database query into a data field on a website. The Illinois AG was notified on July 19.

Open Source Media Coverage

The attackers reportedly were hitting the database five times per second, 24 hours a day from June 23 to Aug. 12. The site was taken down as a precaution on July 13, and firewall protection prevented further data from being compromised. Passwords of election authorities and their staffs reportedly were compromised. Personal information of voters also was compromised, but their voting signatures and histories apparently were not exposed.

State voting systems have been dealing with hacking attempts for 10 years, noted Ken Menzel, general counsel of the Illinois State Board of Elections. However, why hackers targeted Illinois and not other states in this instance is unknown, he told the E-Commerce Times. "Until law enforcement catches the who, I don't think we're going to have a sense of exactly why," Menzel said.

There are about 7.5 million active voters in Illinois, he noted, and 200,000 is the upper end of the number of records compromised. The Illinois Attorney General's office is working with the board to notify voters about the breach, said AG spokesperson Eileen Boyce.

Systems Vulnerable

The exploitation of vulnerabilities in electronic voting systems has been a nagging worry for years. "I think we can safely say that it's a unanimous and universal concern that electoral systems are appropriately protected," said Christopher Budd, global threat communication manager at Trend Micro.

Voting data can be exploited in a number of ways, he told the E-Commerce Times, including extortion, phishing schemes, and identity theft -- particularly involving the deceased.

Department of Homeland Security Secretary Jeh Johnson last month hosted a conference call with top state election officials to discuss the cybersecurity issue and the need to protect voting infrastructures. The call participants included members of the U.S. Election Assistance Commission, the Department of Commerce's National Institute for Standards and Technology, and the Department of Justice.

DHS planned to launch a Voting Infrastructure Cybersecurity Action Campaign, Johnson said during the call, enlisting experts of all levels from the government and private sector. State officials should implement NIST and EAC recommendations on securing voting infrastructure, he advised, which include making sure voting machines are not connected to the Internet while voting is taking place.

The Russian Connection

Meanwhile, Arizona took its voter registration system offline in June, due to what the FBI characterized as a credible threat, according to Matt Roberts, spokesperson for Arizona Secretary of State Michele Reagan. "As you might have seen, a credential used by a county user to access the Arizona Statewide Voter Registration System was compromised by malware inadvertently installed on a county computer and subsequently leaked by a known Russian hacker," he told the E-Commerce Times.

"Our office immediately took steps to perform an exhaustive security review of the statewide voter registration system with the help of the Arizona Department of Administration and our voter registration software vendor," Roberts said. "We found no evidence that anyone was able to penetrate our security

Open Source Media Coverage

to gain access to the information within the registration database," he noted. "We have implemented enhanced measures to ensure access the system is secure, restored the system and continued its use."

The FBI has launched investigations into malicious cyberattacks on the electronic election infrastructures in Illinois and Arizona, and federal officials last month warned states to take steps to protect their systems as the presidential campaign heats up, according to reports that surfaced this week.

The attacks, dating back to June, led to the illegal download of information on more than 200,000 Illinois voters, leading to a 10-day shutdown of the state's voter registration system. Hackers also penetrated systems in Arizona but apparently failed to download specific voter information.

A timeline issued by the Illinois Board of Elections confirmed that it contacted the Illinois Attorney General's office, was contacted by the FBI, and has been cooperating with the agency.

Voter fraud in Arizona: What it looks like, how often it happens and how it is fought

Alexa Chryssovergis, The Republic | azcentral.com Published 7:00 a.m. MT Aug. 14, 2017 | Updated 10:39 a.m. MT Aug. 14, 2017

President Donald Trump has called voter fraud an issue that may have swayed the outcome of the 2016 popular vote. Without proof, he claimed that millions of people voted illegally in the election. Through an executive order in May, he created a Presidential Advisory Commission on Election Integrity. The commission likely could replicate work done in Arizona since 2008. Since that year, state officials have examined hundreds of thousands of cases where someone might have voted twice in an election. After scrutinizing those cases, 30 were sent to the Arizona Attorney General's Office.

Twenty resulted in convictions. The path to those convictions started with the work of the Interstate Voter Registration Crosscheck Program, now run by Kansas Secretary of State Kris Kobach. The program compares voter-roll data state to state. It has a dual purpose: to clean the voter rolls and identify people who are registered in multiple states (likely because they moved), and to find voter fraud. Kobach also is the vice chairman of Trump's commission. Crosscheck finds only cases of double voting; other types of voter fraud include false registrations, forgery and perjury. But the number of other kinds of voter-fraud cases is "far less than the double-voting cases," said Mia Garcia, spokeswoman for Arizona Attorney General Mark Brnovich

What are these cases?

Here are some details of the 30 referrals received by the Attorney General's Office:

- Twenty resulted in convictions.
- Of the others, six cases were turned down, one was dismissed, one conviction was overturned on appeal and two are still active.
- Eleven convictions were in Maricopa County.
- The nine others occurred in Pinal, Santa Cruz, Pima, Mohave, La Paz and Graham counties.

- The average fine for those convicted was a little more than \$5,000. Fines ranged from \$2,500 to \$13,800.
- Most of those convicted received 100 hours of community service, although in two cases, the defendants were ordered to perform 200 and 300 hours.
- A few defendants had their records expunged after paying the court and completing their hours.

Several of these individuals claimed in court documents that they did not intentionally vote twice. Many said they were extraordinarily busy or stressed around the time, and as a result, they don't really recall doing it. Accidental double voting is probably the most common type of voter fraud that occurs, said David Wells, senior political-science lecturer at Arizona State University. Intentional voter fraud is "pretty much nonexistent," Wells said, and not something that sways elections.

"It's just a fraudulent allegation of massive voter fraud that Donald Trump put forward," Wells said. "The basis of this commission is fraudulent." While he didn't agree with Trump's commission or his allegations, Wells said Crosscheck and cleaning voter rolls is important and worthwhile. On this point, Rep. Michelle Ugenti-Rita, R-Scottsdale, agrees. The state representative has taken a strong stance on voter-fraud prevention through some of her proposed legislation. But when asked if she agreed with the basis for Trump's commission or whether his allegations of voter fraud were legitimate, Ugenti-Rita didn't directly answer. "I think that protecting something that's so fundamental to democracy, like fair elections, is essential," she said.

How Crosscheck works

The Arizona Secretary of State's Office initiates the somewhat complex process of identifying double votes. These are the steps:

- Arizona sends voter data, including an individual's first and last name and partial Social Security number, to the Crosscheck program in Kansas. According to Samantha Poetter, director of public information for Kobach, 27 other states last year did the same and 30 are signed up to share this information in coming years.
- A computer program compares states' data.
- Matches are sent to respective secretaries of state offices.
- At the Arizona Secretary of State's Office, signature comparisons begin if it appears an individual submitted two ballots, staff members manually compare signatures on the ballots and determine whether to investigate further.
- The narrowed pool of matches are sent to counties, which perform their own review. They report their findings to the secretary of state.
- If there's a hard match, meaning the first and last name, birth date, Social Security number and signature match on two ballots, the case is referred to the Arizona Attorney General's Office for further review.

"It's a fairly laborious process that does take a great deal of time," said Matt Roberts, spokesman for Arizona Secretary of State Michele Reagan. "And that's why we in the past have announced cases of double voting long after the election occurred."

In 2016, the office received 79,331 matches, which are classified into four types by how strong they are, with 1 being the strongest. Roberts said the number of matches is fairly consistent year after year.

- Type 1: An individual's name, date of birth and partial Social Security number are the same in both records. In 2016, a majority of the matches (65,521) were Type 1.
- Type 2 and 3: One state doesn't have a Social Security number.
- Type 4: Everything is the same in both records except the Social Security number.

How is Crosscheck different?

Most states rejected the Trump commission's initial request for data in some form, though many share similar data with Crosscheck. Many cited privacy concerns after the commission said the data would be made public. Arizona Secretary of State Michele Reagan initially released a statement June 30 saying she would only turn over data that would not violate state privacy laws. But after public outcry, she said she would completely deny the request. The legality of the request still remains unclear. Several groups have brought lawsuits against the commission, so far to no avail. Kobach asked states for the voter data again on July 26, updating the request to say the information would be kept private.

Reagan still has not said whether she will release the information, but Roberts said it's up to lawyers to decide whether anyone can refuse to provide this information now that Kobach has promised it will be kept private. Whether any office can refuse a "perfectly legal public-records request" is something only legal counsel can determine, Roberts said.

The commission has asked all 50 states plus Washington, D.C., for names, addresses, dates of birth, last four digits of Social Security numbers, voter history from 2006 onward and party registrations, among other information. In an email, Poetter said the information collected by Crosscheck differs in some ways from the data requested by the commission. Crosscheck does not ask for several fields that Trump's commission requested, she said, including party affiliation, voter history from 2006 on, canceled status, information on felony convictions, and information on registration in other states, military status and overseas citizen status.

Despite the similarities in many data fields of what Crosscheck collects and what the commission is requesting, Reagan's office has no problem sharing the Crosscheck data because it's kept private. Confidential information, such as partial Social Security numbers, is redacted if shared with the public, Roberts said. Voters in some states are withdrawing their voting registration amid a request from President Trump's voter fraud panel to collect voting data from all 50 states.

Will Trump's commission find something new?

Trump's voting commission has caused a backlash — not just from secretaries of state, but also from non-profit advocacy groups, political-science experts, and former and current government employees, among others. Many have expressed fears that instead of preventing voter fraud, the commission will perpetuate voter suppression. Kobach has received criticism for imposing what some see as restrictive voting practices in Kansas. Kobach and his office did not respond to multiple requests for an interview from *The Arizona Republic* over several weeks. Some of these voting practices are standard in Arizona, such as requiring proof of U.S. citizenship when registering to vote. In Arizona and Kansas, a voter must also show ID at the polls. Trump claimed a large portion of those who voted illegally were people who were not in the country legally. With both stringent voter laws and the Crosscheck program, Arizona has not found thousands, hundreds or even dozens of cases of voter fraud. Instead, the state has convicted 20 people of double voting, and even fewer of other kinds of voter fraud.

One big question remains: When Trump's commission releases its findings, what more might emerge about voting problems in Arizona? "I think the commission's intent to improve electoral integrity could take a great number of directions," Roberts said. "Perhaps maybe the commission could take a look at some of the things we're doing and suggest that other states do them as well."

READ MORE:

[Arizona GOP sends ominous email seeking 'voter' info](#)

[Voting fraud? Not here, Arizona election officials say](#)

[Are undocumented immigrants voting illegally in Arizona?](#)

[Trump commission again asks Arizona to release voter data](#)

California

State Election and Cybersecurity Officials



ALEX PADILLA SECRETARY OF STATE, CALIFORNIA

BIO

Alex Padilla was sworn in as California Secretary of State on January 5, 2015. He is committed to modernizing the office, increasing voter registration and participation, and strengthening voting rights.

Padilla previously served in the California State Senate (2006-2014) where he chaired the Committee on Energy, Utilities, and Communications. As chair, he shepherded legislation to combat climate change and create a greener and more sustainable economy. He pursued an ambitious agenda in the areas of renewable energy, energy efficiency, smart grid, and broadband deployment.

Padilla's parents emigrated from Mexico and raised their family in the working class community of Pacoima, California. His father worked as a short order cook and his mother cleaned houses. Padilla attended local public schools and went on to graduate from the Massachusetts Institute of Technology with a bachelor's degree in Mechanical Engineering. He recently completed a five-year term as a member of the MIT Corporation (Board of Trustees). Padilla is often asked how he moved from engineering to public service. He explains that in many ways they are similar; the goal of each is solving problems.

State Election and Cybersecurity Officials

After working for Hughes Aircraft in Southern California, Padilla participated in the Coro Fellows Program where he received leadership and public affairs training. He would later work for U.S. Senator Dianne Feinstein and then-Assembly member Tony Cardenas.

In 1999, at the age of 26, Padilla was elected to the Los Angeles City Council to represent the same east San Fernando Valley community where he grew up. In 2001, his colleagues elected him to the first of three terms as Council President, becoming the youngest member and the first Latino to serve in this capacity.

As Council President, Padilla provided citywide leadership at critical times. He was Acting Mayor during the tragedy of September 11, 2001. He assisted in the interview and selection of William Bratton as Chief of Police and helped negotiate the approval of LA Live and the modernization of Los Angeles International Airport.

In 2005, Padilla was elected President of the League of California Cities. He advocated on behalf of California cities in the State Capitol and fought to protect their budgets and advance their legislative priorities.

In 2006, Padilla was elected to the California State Senate. He was reelected in 2010. Over the course of eight years, Padilla established a diverse and groundbreaking legislative record.

To address the growing rates of obesity and diabetes, Padilla authored the law that made California the first state in the nation to require chain restaurants to post calorie information directly on menus and menu boards. "Menu labeling" was later included in the Affordable Care Act and is now national policy.

Padilla also authored California's first smoke free housing law and fought to increase enforcement and penalties for the illegal sale of tobacco to minors. He also established a sustainable funding source for pediatric trauma care throughout the state.

When he learned that thousands of cell phones were being smuggled into state prisons and used to direct criminal gang activity in our communities, Padilla led efforts to stop it. He wrote the law that criminalized the transfer, sale, or possession of illicit cell phones in prison. He also authored the law that prohibits violent felons from possessing, buying, or transferring body armor such as bulletproof vests.

There are approximately 1.5 million English Learners in California public schools. One in four k-12 students and about forty percent of all kindergarten students are English Learners. Sadly, only about eleven percent of English Learners achieve English proficiency and earn reclassification each year. Padilla authored a series of legislative measures to identify and implement best practices in English Learner curriculum and instruction statewide. He also advocated for funding reform and accountability for schools and school districts with high concentrations of English Learner students.

Through research and legislative hearings, Padilla exposed a bottleneck in the college transfer process. He wrote the law that streamlined the transfer process and created a clear and consistent pathway for community college students working to transfer to the California State University system. Padilla also authored the law that requires California's elite university athletic programs to provide alternative scholarships to student-athletes who lose their athletic scholarships due to injury.

With the potential to create 20,000 jobs, Padilla authored key legislation to facilitate the construction of a new convention center and carbon-neutral sports stadium in downtown Los Angeles. With the goal of modernizing and better managing freight and passenger rail between San Diego, Los Angeles, and San Luis Obispo, he wrote the law to establish a joint powers authority to better govern the nation's second busiest rail corridor.

State Election and Cybersecurity Officials

As an engineer, Padilla is committed to the promise of science and advanced technology. To address concerns about the misuse of genetic information, Padilla authored the California Genetic Information Non-discrimination Act. To reduce the number of injuries and fatalities on our roads, he authored the law requiring safety and performance standards for autonomous ("driverless") vehicles. And, working with seismologists at CalTech, U.C. Berkeley, and the U.S. Geological Survey, Padilla authored a bill requiring the state to create a statewide Earthquake Early Warning System.

Padilla previously served as President of the National Association of Latino Elected and Appointed Officials (NALEO), a non-partisan organization made up of more than 6,000 federal, state, and local officials dedicated to all aspects of civic engagement.

Padilla lives with his wife Angela and their three sons in the San Fernando Valley.



MARK GHILARDUCCI
DIRECTOR OF EMERGENCY OPERATIONS, CALIFORNIA

BIO

With more than 25 years of service in emergency management, Mark Ghilarducci was appointed director of the California Office of Emergency Services (Cal OES) by Governor Jerry Brown in February 2012.

Ghilarducci received a Bachelor of Science degree in physiology in 1987 from the University of California, Davis, before becoming deputy fire chief in charge of special operations for Cal OES's predecessor, the Office of Emergency Services (OES), from 1988 to 1997. He is a 1998 graduate of the Fellowship Program for Senior Executives in State and Local Government at Harvard University, John F. Kennedy School of Government.

Ghilarducci moved from state to federal government and was a coordinating officer in District IX at the Presidio of San Francisco for the Federal Emergency Management Agency (FEMA) from 1997 to 2000 and then returned to state government as deputy director for OES from 2000 to 2003. He left government service in 2003 to join Witt Associates, a public safety and crisis management consulting firm based in Washington, D.C., as west regional vice president. In 2011, Ghilarducci moved to Diamante Partners LLC, an administrative management and general management consulting services company in Folsom, California, as partner and managing director.

State Election and Cybersecurity Officials



EDMUND G. BROWN, JR.
GOVERNOR, CALIFORNIA

BIO

Edmund G. Brown Jr. was born in San Francisco on April 7, 1938. He graduated from St. Ignatius High School in 1955 and entered Sacred Heart Novitiate, a Jesuit seminary. He later attended the University of California, Berkeley, graduating in 1961 before earning a J.D. at Yale Law School in 1964.

Brown was elected Trustee for the Los Angeles Community College District in 1969, Secretary of State in 1970 and Governor in 1974 and 1978. As Governor, he helped create millions of jobs, strengthened environmental protections and promoted renewable energy. After his governorship, Brown lectured and traveled widely, practiced law, served as chairman of the state Democratic Party and ran for president.

In 1998, Brown was elected Mayor of Oakland and helped revitalize its downtown and reduce crime, while also founding two high-performing charter schools. Brown was elected California Attorney General in 2006 and worked to protect consumers, pursue mortgage fraud and real estate scams, champion workers' rights and crack down on violent crime.

State Election and Cybersecurity Officials

Brown was elected to a third gubernatorial term in 2010 and to a historic fourth term in 2014. Since returning to the Governor's Office, Brown helped eliminate the state's multi-billion budget deficit, spearheading successful campaigns to provide billions in new funding for California's schools (Proposition 30) and establish a robust Rainy Day Fund to prepare for the next economic downturn (Proposition 2).

Under Brown, California has cut its unemployment rate in half, expanded health coverage to millions more Californians, and added more than 2 million new jobs, while enacting sweeping public safety, immigration, workers' compensation, water, pension and economic development reforms. California has also established nation-leading targets to protect the environment and fight climate change, and by 2030 the state will: reduce greenhouse gas emissions 40 percent below 1990 levels, generate half of its electricity from renewable sources, double the rate of energy efficiency savings in its buildings and reduce today's petroleum use in cars and trucks by up to 50 percent.

Brown is married to Anne Gust Brown, who serves as Special Counsel, an unpaid position, in the Office of the Governor.

Election Infrastructure Information

Counties: 58

Voter Registration: All voters must register. The deadline to register is 15 days prior to Election Day.

Voter Qualifications: A United States citizen and a resident of California; 18 years old or older on Election Day; not currently in state or federal prison or on parole for the conviction of a felony; and not currently found mentally incompetent to vote by a court.

Voter Equipment used to cast ballots: Voters may cast ballots by mail or in person. When voting in person, voters are provided a paper ballot, unique passcode, or computer memory card, depending on the voting system used by the county in which they vote.

California Voting Systems Standards, California Secretary of State, October 2014

1.3.2 Types of Voting Systems

HAVA Section 301 and the California Elections Code define a voting system as the total combination of mechanical, electromechanical, or electronic equipment (including the software, firmware, and documentation required to program, control, and support the equipment), that is used to define ballots; to cast and count votes; to report or display election results; and to maintain and produce any audit trail information. In addition, a voting system includes the practices and associated documentation used to identify system components and versions of such components; to test the system during its development and maintenance; to maintain records of system errors and defects; to determine specific system changes made after initial certification; and to make available any materials to the voter (such as notices, instructions, forms, or paper ballots).

In addition to defining a common set of standards that apply to all voting systems, the Standards identify requirements specific to a particular type of voting system, where appropriate. However, the Standards recognize that as new solutions and technology continues to evolve, the distinctions between voting system types may become blurred. The Standards contain appropriate procedures to ensure new developments provide the necessary integrity and can be properly evaluated in the certification process.

Consequently, manufacturers that submit a system that integrates components from more than one traditional system type or a system that includes components or technology not addressed in the Standards **shall** submit the results of all beta tests of the new system when applying for certification. Manufacturers **shall** also submit a proposed test plan for use in certification testing. The Standards permit manufacturers to produce or utilize interoperable components of a voting system that are tested within the full voting system configuration.

The listing below summarizes the functional requirements that HAVA Section 301 and California Election Code mandates to assist voters. While these requirements may be implemented in a different manner for different types of voting systems, all types of voting systems must provide these capabilities:

- Permit the voter to verify (in a private and independent manner) the vote selected by the voter on the ballot before the ballot is cast and counted
- Provide the voter with the opportunity (in a private and independent manner) to change the ballot or correct any error before the ballot is cast and counted
- Notify the voter if he or she has selected more than one candidate for a single office, inform the voter of the effect of casting multiple votes for a single office, and provide the voter an opportunity to correct the ballot before it is cast and counted
- Be accessible for individuals with disabilities in a manner that provides the same opportunity for access and participation (including privacy and independence) as for other voters
- Provide alternative language accessibility pursuant to Section 203 of the Voting Rights Act and California Elections Code section 14201

Election Infrastructure Information

Excerpts from California Elections Code regarding voting security:

All precinct board members must attend a training class on the use of voting machines and other precinct responsibilities unless appointed to fill an emergency vacancy. (§ 19340.)

All voting equipment shall be transferred to the polling places in charge of an authorized official, who shall certify to their delivery in good order. (§ 14112.) Ballots and all other election supplies appropriate to the system will also be provided. (§§ 14113, 14300.)

Before or as soon as the polls are closed, unless otherwise directed by the county elections official, the precinct board shall remove the voted ballots from the ballot container and take them out of the secrecy envelopes or detach them from the secrecy stubs. Where the envelope or stub is also the write-in ballot, and a write-in vote has been registered thereon, the ballot card shall not be separated from the envelope or stub. If two or more separate ballot cards have been used in the election, the precinct board shall sort them into groups, each of which shall contain the same series of ballot cards. (§ 14420(a), (c).) After completing the foregoing step, the precinct board shall count the number of ballot cards in each group, and certify the number of ballots cast on the voting roster as provided by Section 14107. If there is any discrepancy between the number of voters listed in the roster and the number of ballots voted, this fact shall be noted with an explanation of the difference and signed by all members of the precinct board. (§ 14420(b).) (See Section [IV. Election Day](#) for more information on procedures after the close of the polls.)

The precinct board shall group voted ballot cards and voted separate write-in ballots, as directed by the elections official, and place them in containers. The board shall also place spoiled and void ballots, if any, in containers as directed by the elections official. All of these ballots, along with the containers for voted ballot cards, shall be placed in one or more boxes, which shall then be sealed and delivered as soon as possible to the receiving centers or central counting places with the unused ballots, supplies, and other materials as directed by the elections official. (§ 14421.)

If votes are cast by means of a voting machine, the statement of the result of votes cast, which shall be certified by the precinct board, shall contain certain information, including certificates which shall be signed by the election officers before the polls are opened and which shall be filled out after the polls have been closed. (§ 19380.)

If votes are cast by means of a voting machine, as soon as the polls are closed, the precinct board, in the presence of the watchers and all others lawfully present, shall immediately lock the voting machine against voting and do all of the following: (1) Count the votes cast on voting machines and report the results. (2) Complete, sign, and return to the elections official all furnished forms requiring its signatures. When votes are counted on one or more voting machines at the precinct, all members of the precinct board, upon the completion of their duties, shall sign a certificate of performance. (§§ 15250, 15250.5.) (See Section [V. Canvassing the Vote](#) for more information.)

Each qualified political party may employ, and have present at the central counting place or places, not more than two representatives to check and review the preparation and operation of the tabulating devices, their programming and testing, and have the representatives in attendance at any or all phases of the election. (§ 15004(a).)

Election Infrastructure Information

Any bona fide association of citizens or a media organization may employ, and may have present at the central counting place or places, not more than two representatives to check and review the preparation and operation of the tabulating devices, their programming and testing, and have the representatives in attendance at any or all phases of the election. (§ 15004(b).)

The county elections official may limit the total number of representatives of bona fide associations of citizens or media organizations in attendance to no more than 10 by a manner in which each interested bona fide association of citizens or media organization has an equal opportunity to participate. Any representative of a qualified political party employed and in attendance shall not be subject to this limit. (§ 15004(c).)

Voting System Security

Election security is a major concern at all levels of government. The end goal of election security is to deliver a process that is not only safe and secure, but also fair, accurate and accessible. In California, at both the state and county level, there are a multitude of layered security protocols in place.

At the state level, the Secretary of State's Office (SOS) is legally mandated to certify any voting system prior to its sale and use within California. As a result, the state has developed one of the most strenuous voting system testing and certification programs in the country. New voting systems applying for certification must undergo months of extensive testing which includes;

- Examination and testing of system software;
- Software source code review and evaluation;
- Hardware and software security penetration testing;
- Hardware testing under conditions simulating the intended storage, operation, transportation, and maintenance environments;
- Inspection and evaluation of system documentation; and
- Operational testing to validate system performance and functioning under normal and abnormal conditions.

SOS also requires all voting systems be capable of deployment with dual-installation architecture ("air gapping"). This process physically separates two installations and all associated devices, establishing an air gap. The separation of installations aids in protecting against the propagation of viruses.

In addition, SOS mandates voting system vendors, security consultants and county officials follow strict chain of custody requirements for voting system software and hardware throughout the testing and certification process. Upon certification of a system, the "trusted build" is held in a secure location and all distributed copies of the trusted build are hand delivered by SOS staff to the recipient county officials.

At the local level, California counties are required to abide by stringent sets of rules and regulations regarding implementation and use of a voting system. A few notable rules and regulations include; performance of logic and accuracy testing on voting systems prior to each election and ensuring specific procedures for programming, deployment and use of voting equipment during elections are met.

Additionally, pursuant to Elections Code section 19205, no part of a voting system shall be connected to the internet at any time. Nor shall any part of a voting system electronically receive or transmit election data through an exterior communication network of any type.

Election Infrastructure Information

Ballots cast in California are primarily cast on paper ballots. Historically, it has been asserted that paper trails associated with paper ballots allow for prompt detection of possible intrusions into the voting process. Therefore, voting systems that are direct record electronic systems must have the ability to provide a voter verified paper audit trail (VVPAT) for audit, recount, and manual tally purposes. Further, as a safeguard to ensure votes were accurately read and tallied, county elections officials are required to conduct a manual tally of one percent of the precincts as part of the official canvass of election results.

Voting System Approval

Under California law, a voting system and any modification to a voting system must be approved by the Secretary of State before it can be used in any election.

When a voting system is brought to California for review, the Secretary of State conducts a thorough examination and review of the proposed system that includes:

- Review of the application and documentation;
- End-to-end functional examination and testing;
- Volume testing under election-like conditions of all voting devices used by the voter;
- Security testing that includes a full source code review and penetration testing;
- Accessibility examination and testing; and
- Public hearing and public comment period.

The Secretary of State's examination and review process is designed to test the system for compliance with the California Voting System Standards. Here is a summary of the key differences between the EAC and California processes:

Description	EAC	California
Application & Documentation	A technical data package (TDP) is submitted by the vendor to the EAC. The TDP identifies the voting system design, operation, functionality, hardware, software, security, maintenance, and other system requirements.	The California Voting System Standards section 9 describes the technical data package that shall be submitted by the vendor.
Software	Examines system source code for its compliance with the EAC's Voluntary Voting System Guidelines (VVSG).	Examines system source code for compliance with the California Voting Systems Standards.
Security	Determines if the system can detect, prevent, log and recover from a broad range of security risks.	Examines the system for compliance with California Voting Systems Standards.
Hardware	Evaluates whether the voting system hardware can withstand exposure to environmental conditions, including varying and extreme temperatures, humidity, vibrations, and inconsistent voltage.	Evaluates the hardware to the California Voting System Standards.
Functional	Determines if the voting system can perform each function required by federal law.	Determines if the voting system can perform to the standards required by the California Voting System Standards.
Accessibility	Requires vendor to provide the EAC with results from third-party accessibility testing.	Independently contracts with third-party accessibility experts to conduct accessibility testing.

Election Information

Primary Election: June 5, 2018

General Election: November 6, 2018

Upcoming Local Elections

Election Date	<u>Voter Registration</u>	<u>Vote-by-Mail Ballot Request</u>	Completed Ballots, Including Vote-by-Mail Ballots
<p>August 22, 2017, San Luis Obispo County</p> <p>7:00 a.m. to 8:00 p.m.</p>	<p><u>Online</u> or Postmark by August 7, 2017</p> <p>or</p> <p>You can “<u>conditionally</u>” register and vote at your county elections office after the 15-day voter registration deadline.</p>	<p>Must arrive by August 15, 2017</p>	<p>Personally delivered ballots: Must be delivered by close of polls on August 22, 2017;</p> <p>Mailed ballots: Must be postmarked on or before August 22, 2017, and received by your county elections office no later than September 1, 2017.</p>
<p>August 29, 2017, Multiple counties</p> <p>7:00 a.m. to 8:00 p.m.</p>	<p><u>Online</u> or Postmark by August 14, 2017</p> <p>or</p> <p>You can “<u>conditionally</u>” register and vote at your county elections office after the 15-day voter registration deadline.</p>		

Assembly District 51* - Special Election

*Wholly contained within Los Angeles county

Election Information

Election Date	<u>Voter Registration</u>	<u>Vote-by-Mail Ballot Request</u>	Completed Ballots, Including Vote-by-Mail Ballots
<p>October 3, 2017, Assembly District 51 - Special Election</p> <p>7:00 a.m. to 8:00 p.m.</p>	<p><u>Online</u> or Postmark by September 18, 2017</p> <p>or</p> <p>You can “<u>conditionally</u>” register and vote at your county elections office after the 15-day voter registration deadline.</p>	<p>Must arrive by September 26, 2017</p>	<p>Personally delivered ballots: Must be delivered by close of polls on October 3, 2017; Mailed ballots: Must be postmarked on or before October 3, 2017, and received by your county elections office no later than October 6, 2017.</p>

Statewide Direct Primary Election - June 5, 2018

Election Date	<u>Voter Registration</u>	<u>Vote-by-Mail Ballot Request</u>	Completed Ballots, Including Vote-by-Mail Ballots
<p>June 5, 2018, Statewide Direct Primary Election</p> <p>7:00 a.m. to 8:00 p.m.</p>	<p><u>Online</u> or Postmark by May 21, 2018</p> <p>or</p> <p>You can “<u>conditionally</u>” register and vote at your county elections office after the 15-day voter registration deadline.</p>	<p>Must arrive by May 29, 2018</p>	<p>Personally delivered ballots: Must be delivered by close of polls on June 5, 2018; Mailed ballots: Must be postmarked on or before June 5, 2018, and received by your county elections office no later than June 8, 2018.</p>

Open Source Media Coverage

[Forty-four states and DC have refused to give certain voter information to Trump commission](#)

By Liz Stark and Grace Hauck, CNN

Updated 5:49 AM ET, Wed July 5, 2017

California: "I will not provide sensitive voter information to a commission that has already inaccurately passed judgment that millions of Californians voted illegally. ..." Secretary of State Alex Padilla said in a [statement](#) Thursday. "California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud made by the President, the Vice President, and Mr. Kobach. The President's Commission is a waste of taxpayer money and a distraction from the real threats to the integrity of our elections today: aging voting systems and documented Russian interference in our elections."

[How states are handling Trump's voter information request](#)

- By The Associated Press
- Aug 9, 2017.

These are state-by-state responses to a request for detailed voter data from President Donald Trump's Presidential Advisory Commission on Election Integrity, which is investigating voter fraud. The information indicates whether a state is willing to comply with, is denying or is undecided on the request for data. Some of the states that are willing to comply have fees or other requirements of the commission. All states that have agreed to provide the information are withholding some details that the commission said it wanted only if it was considered public under state law. The commission sent one request in late June and another in July after a court said the data collection could move ahead.

CALIFORNIA

Deny

Secretary of State Alex Padilla, a Democrat, reiterated his refusal to provide information to the commission on July 26. "The commission's new request does nothing to address the fundamental problems with the commission's illegitimate origins, questionable mission or the preconceived and harmful views on voting rights that many of its commissioners have advanced," he said in a statement. "Let me reassure voters: I will not provide this commission with Californians' personal voter data. I will continue to do everything in my power to protect California citizens' ability to exercise their rights to register and vote free of barriers and intimidation."

State Election and Cybersecurity Officials



SCOTT NAGO
CHIEF ELECTIONS OFFICER, HAWAII

BIO

???????



DAVID Y. IGE

GOVERNOR, HAWAII

BIO

Governor David Y. Ige was sworn in as the eighth governor of the State of Hawai‘i on December 1, 2014. He became the fourth native-born Governor of Hawai‘i and first governor in the United States of America of Okinawan descent. Gov Ige Aloha Shirt HI Res Governor Ige was born and raised in Pearl City and is the fifth of six sons of Tokio and Tsurue Ige. Governor Ige attended public schools in Pearl City – Pearl City Elementary School, Highlands Intermediate School, and Pearl City High School. He also participated in community sports, beginning with eight years of playing in the Pearl City Little League. At the newly built Pearl City High School, Governor Ige excelled in many activities. In his junior year, he was elected Student Body Vice President, and he served as Senior Class President the following year. He also led his varsity tennis team to a championship and was honored as the “Scholar-Athlete of the Year.” He graduated fifth in his class of more than 500 students in 1975. Governor Ige then attended the University of Hawai‘i at Mānoa, where he earned a Bachelor of Science degree in Electrical Engineering. While at UH, he served as Student Body Secretary and an officer of several honor societies as well as Treasurer and Vice-President of his fraternity, Phi Delta Sigma. Most importantly, UH is where Governor Ige met his wife, Dawn Amano-Ige.

After college, while working for GTE Hawaiian Tel a career that spanned 18 years, Governor Ige took graduate courses at UH and earned a master of Business Administration degree in Decisions Sciences. In 1986, Hawaii Business magazine named him one of the university’s Top 10 MBA students. He went on to become a successful electrical engineer and project manager with a 34-year career devoted to information technology, telecommunications, networks, and responsible public policy. Prior to being elected governor of Hawai‘i, he served as Program/Project Manager with Robert A. Ige and Associates, Inc., Vice President of Engineering at NetEnterprise, and Project Engineer/Senior Principal Engineer at Pihana Pacific, which established the first world-class data center and carrier-neutral Internet exchange in Hawai‘i and the Pacific.

Governor Ige began his political career in 1985 after being appointed by then Governor George Ariyoshi to fill a vacant seat in the Hawai‘i House of Representatives. In 1994, then Representative Ige was elected to the Hawai‘i Senate where he represented his home district of ‘Aiea / Pearl City until 2014. During his legislative career, Governor Ige served as the chairman of nine different committees which included the committees on Education, Health, and Ways and Means.

Election Infrastructure Information

Counties: 5

Voter Registration: All voters must register. You must register no later than: 30 days before the election, if you're completing a standard voter registration. 7 days before the election, if you're applying for permanent absentee voting..

Hawaii Election Infrastructure Information

Voter Qualifications: A United States citizen and a resident of California; 18 years old or older on Election Day; not currently in state or federal prison or on parole for the conviction of a felony; and not currently found mentally incompetent to vote by a court.

Voter Identification: Voters in Hawaii must present a valid form of identification at the polls. This identification does not have to include a photo of the voter. According to the National Conference of State Legislatures, valid forms of ID in Hawaii include driver's licenses, state ID cards, utility bills, bank statements, and other government-issued documents.

Voter Equipment used to cast ballots: Voters may cast ballots by mail or in person. When voting in person, voters are provided a paper ballot, unique passcode, or computer memory card, depending on the voting system used by the county in which they vote.

State Requirements and the Federal Voting System Testing and Certification Program

No Federal Requirements-The Chief Election Officer adopts voting systems for use in HI elections.

Applicable Statute(s)-“The chief election officer may adopt, experiment with, or abandon any voting system authorized under this chapter or to be authorized by the legislature. These systems shall include, but not be limited to voting machines, paper ballots, and electronic voting systems. All voting systems approved by the chief election officer under this chapter are authorized for use in all elections for voting, registering, and counting votes cast at the election.” HAW. REV. STAT. § 16-1 (2008). “All voting systems adopted under this chapter by the chief election officer of the legislature shall satisfy the following requirements: (1) It shall secure to the voter secrecy in the act of voting; (2) It shall provide for voting for all candidates of as many political parties as may make nominations, nonpartisans, and for or against as many questions as are submitted; (3) It shall correctly register or record and accurately count all votes cast for any and all persons, and for or against any and all questions.” HAW. REV. STAT. § 16-2 (2008).

Applicable Regulation(s)-“The chief election officer or designated representative shall approve all necessary forms, supplies, and procedures used in the operation of any voting system after consultation with the respective clerks.” HAW. CODE R. § 2-54-1 (Weil 2008).

State Certification Process-The chief election officer determines whether a voting system may be used in state elections. During the examination, the chief elections officer must verify that the voting systems are safe, secure, and accurate. HAW. REV. STAT. § 16-2 (2008).

Fielded Voting Systems-After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document.

Election Infrastructure Information

The voting machine systems used in Hawaii are optical scan and DRE.

Hawaii Election Infrastructure Information

Voting Machines

Optical Scan: With this system, you will receive a card or sheet of paper, which you take over to a private table or booth. The card has the names of the various candidates and ballot measures printed on it. With a pen or pencil you fill in a little box or circle or the space between two arrows. When you are finished filling out all the cards, you may bring the cards over to a ballot box, where poll workers will show you how to put the cards in the box. Or in some places, you may feed the completed cards or papers into a computer device that checks your card or paper right there at the polling place to make sure you have voted the way you want to and counts the votes.

Direct Recording Electronic (DRE): This is the newest kind of system in use in the U.S. All the information about who and what you are voting for is on an electronic screen like a TV or computer screen.

There are many variations of DREs because lots of companies are inventing new ones, and many cities, counties and states are trying them out. Usually, after you have signed in, the poll workers will give you a card that you slide into a device to start your voting session.

Some of these devices will show all of the candidates and ballot choices on one big screen. Often, with these big screen devices you push a button next to the name of the candidate you want to vote for (or yes or no on a ballot measure). On other DREs, the screen is set up to show pages. On each screen or page, there will probably be one thing to vote on. For example, on one screen or page, you might vote for president. Then you might move to the next page to vote for senator. Often these small-screen devices have a touch screen, where you touch the screen next to the name of the person you want to vote for. Other devices have a key pad. And some have a keyboard, so you can write in the name of someone you want to vote for.

You let the system know you are finished voting by pushing a button, touching the screen or entering something on a keypad.

Hawaii Election Infrastructure Information

Primary Election: August 11, 2018

General Election: November 6, 2018

Primary Election

Election Date	<u>Voter Registration</u>	<u>Vote-by-Mail Ballot Request</u>	Completed Ballots, Including Vote-by-Mail Ballots
August 11, 2018,	July 12, 2018 Voter Registration Ends: Last day to register to vote for the Primary Election with the Clerk's Office or	August 4, 2018 Absentee Ballot Request deadline - By Mail: Last day to request a mail ballot for the Primary Election	November 3, 2018 Early Voting/In Person Absentee voting ends: Close early walk-in voting locations and late registration for the General Election
November 6, 2018	October 8, 2018 Voter Registration Ends: Last day to register to vote for the General Election with the Clerk's Office. Voters are eligible for late registration for the General Election at an early walk-in voting location	September 21, 2018 Absentee Ballot Request deadline - UOCAVA citizens: Mail General Election ballots to overseas voters October 30, 2018 Absentee Ballot Request deadline - By Mail: Last day to request a mail ballot for the General Election from the Clerk's Office	

How states are handling Trump's voter information request

- Governors Press Release
- July 3, 2017

Governor Iges Statement on the request for voter roll data from the Presidential Advisory Commission on Election Integrity

The State of Hawaii has received no request for voter roll data from the Presidential Advisory Commission on Election Integrity. Taking a look at what other states have received, I'm skeptical. At this point, we have no assurance that personal information would be secured. It also appears that the commission aims to address voter fraud. By all accounts, incidents of actual voter fraud are extremely rare. I'm concerned this type of investigation would lead to a denial of voter access. When we get the request, I will share my concerns with state and county elections officials.

- By the Associated Press
- Aug 9, 2017.

These are state-by-state responses to a request for detailed voter data from President Donald Trump's Presidential Advisory Commission on Election Integrity, which is investigating voter fraud. The information indicates whether a state is willing to comply with, is denying or is undecided on the request for data. Some of the states that are willing to comply have fees or other requirements of the commission. All states that have agreed to provide the information are withholding some details that the commission said it wanted only if it was considered public under state law. The commission sent one request in late June and another in July after a court said the data collection could move ahead.

HAWAII

Undecided

Scott Nago, elections chief for Hawaii, said July 24 that his office still has not received an official request. He said the Trump administration sent the request to the lieutenant governor's office, which is not responsible for elections in Hawaii. Nago also said his office received an email saying to hold off on sending the data because of lawsuits. Nago said if the elections office does receive the request, he will then forward it on to the county clerks, who are responsible for the information. According to state law, the counties would be able to release the voter's name, precinct and voting status — meaning whether the voter is active or inactive — because those details are public record, Nago said. But the voters' address, Social Security number, driver's license number, mailing address and voting history would not be released.

December 2, 2016 Elections Commission Meeting

Status of Operations Report from the Chief Election Officer, discussion and action, if appropriate

CEO Nago reported that the Office of Elections (OE) conducted the General Election on November 8, 2016. The deadline to file an election contest with the Supreme Court was Monday, November 28, 2016, which has since passed. There were no contests filed, therefore the election has been certified.

In regards to issues on General Election Day, CEO Nago stated that the control center in Honolulu was understaffed, which caused long wait times for precinct workers to have their phone calls answered. CEO Nago explained that it is becoming increasingly difficult to recruit control center operators, and that there was a high drop-off rate the week before the election. He said that OE will need to examine their procedures for recruiting and staffing the control center so that this does not happen again.

In addition, there were 20 voting machine incidents statewide, with two occurring on the neighbor islands and the rest on Oahu. CEO Nago stated that many of these issues were attributed to things like paper ballot jams and ballot boxes getting full. In these situations, the proper procedure requires the precinct workers to collect the voted ballots into a secure container and scan them when the machines are repaired. CEO Nago said however that there were reports of precinct workers incorrectly depositing voted ballots into unsecure containers, in which case the chairperson was alerted immediately to correct the procedure. CEO Nago explained that the long lines and ballot jams could also be attributed to the two-card ballot on Oahu; voters often did not wait for the first card to be properly scanned before feeding the second card, which caused the machines to jam.

For the upcoming legislative session, CEO Nago reported that OE will be introducing four bills relating to: all-mail elections, automatic voter registration, increasing the fine on the Class C felony for voter fraud from \$1,000 to \$10,000, and removing the requirement for signatories to provide the last four digits of their SSN on candidates' nomination papers.

Commissioner King asked CEO Nago if the workers in the control center are volunteers. CEO Nago said that they are, and clarified that the control center operators are responsible for assisting all polling place workers with any extraordinary issues that may arise.

Commissioner Orikasa asked CEO Nago to confirm that this is not the first time OE will be submitting legislation relating to all mail voting. CEO Nago verified that OE has submitted the same bill several times in the past; during the last two sessions the bill got all the way to the last stage, conference, but did not pass in the end. Commissioner Orikasa said that it does not seem like there is great support in passing the all mail bill, to which CEO Nago responded that they will continue to keep trying.

Commissioner Berg recalled that CEO Nago was going to follow up on some issues after the Primary Election regarding policies for precinct workers. She asked CEO Nago if these procedures have been incorporated into the training manuals. CEO Nago responded that OE does not reprint manuals between the primary and general elections of the same year, but that all procedures are examined so that the manuals can be improved for the following election.

Commissioner Berg asked CEO Nago if OE is working on their response to the Legislature regarding the online voter registration system. CEO Nago confirmed that they are working on their response, which is due 20 days

Hawaii Election Infrastructure Information

prior to the start of the legislative session. Commissioner Berg recalled that OE was also working on another legislative task; CEO Nago said that they will be working on the Hawaii Administrative Rules during the off-session in between elections. Chair Anderson stated that during this upcoming legislative session, his main goal is to get the all mail bill passed. He said that in the last few weeks, he has met with six legislators who are key in passing this bill, and found that they have no objections. Chair Anderson urged the rest of the EC members to meet with their local legislators, and said that they could be provided with a summary sheet that highlights the benefits of all mail elections. He added that all mail voting would eliminate various issues that occurred on General Election Day, including the long lines and the machine jams.

Commissioner Takenaka asked CEO Nago how much it would cost to implement all mail voting. CEO Nago explained that OE is proposing that it be implemented in phases by county, and that once it is completely carried out, there will be an estimated savings of \$800,000 per election cycle.

Commissioner Bates stated that he had visited precincts through Kihei, Lahaina, and East Maui, and observed that the precinct workers were having difficulty getting through to the county clerk's office to verify voter information.

Commissioner Bates said these issues were causing long wait times and some disgruntled voters, which he shared with Maui County Clerk, Mr. Danny Mateo and staff after the election. CEO Nago stated that the same issue occurred in Honolulu with the control center, and that they will need to increase recruitment in order to avoid the same issues next time.

Commissioner Steffey asked CEO Nago if the ballot scanning machines are repaired by someone from the machine's company when there are issues on Election Day, to which CEO Nago confirmed that they are.

Commissioner Steffey said that he had not heard much of anything regarding volunteering for the election aside from an informational pamphlet at the elections office in Kona. CEO Nago explained that the neighbor islands were well staffed and did not experience those same issues that occurred on Oahu.

He added that OE had made additional efforts in Honolulu to recruit volunteers between the primary and general elections by presenting at Neighborhood Board meetings and posting flyers throughout the community.

Commissioner Orikasa asked CEO Nago what percentage of voters are absentee and how this number compares to those of the last couple of elections. CEO Nago responded that 53% of people voted prior to Election Day, which includes absentee and early walk-in ballots. He added that the percentage increased only slightly from a couple of years ago, due to an increase in voter registration.

Commissioner Bates pointed out that many students from Seabury Hall on Maui were precinct volunteers; CEO Nago stated that the county clerks make a conscious effort to recruit staff for the polling places, many of whom are students.

<http://elections.hawaii.gov/wp-content/uploads/2017/03/2016-12-02-EC-Regular-Meeting-Minutes-FINAL.pdf>

NPPD Field-Based Engagement with State Chief Election Officials

North Dakota

Table of Contents

1. **[State Election and Cybersecurity Officials](#)**
2. **[Election Infrastructure Information](#)**
3. **[2018 Elections Information](#)**
4. **[NPPD Talking Points Information](#)**
5. **[Open Source ND Media Coverage](#)**
6. **[OCIA – Election Infrastructure Cyber Risk Characterization](#)**

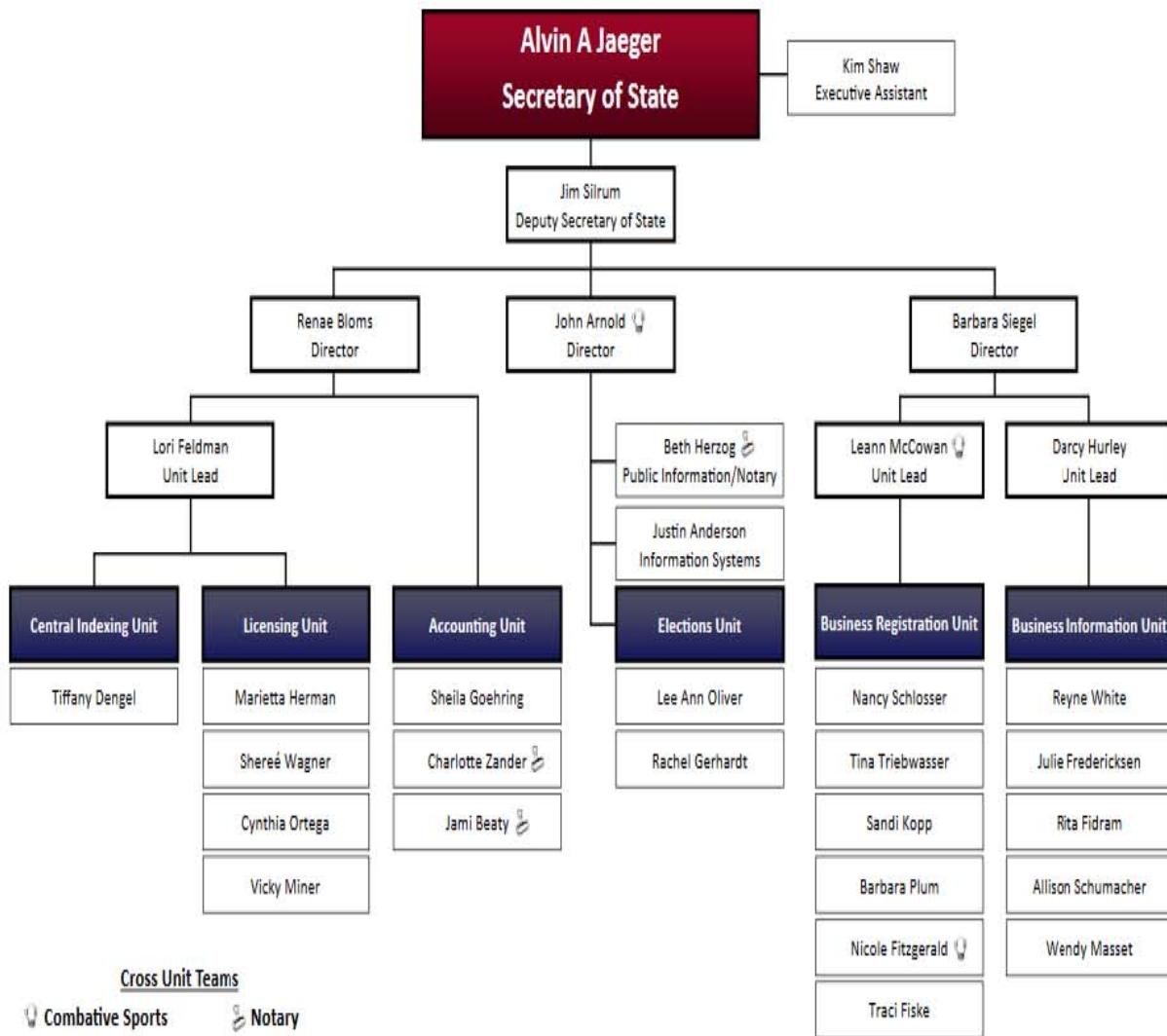
-----**Leave Behind Materials**-----

7. **[NPPD Frequently Asked Questions](#)**
8. **[NASS Elections Security Plan and DHS Assistance Offerings](#)**
9. **[Homeland Security Resource Guide – Election Infrastructure](#)**

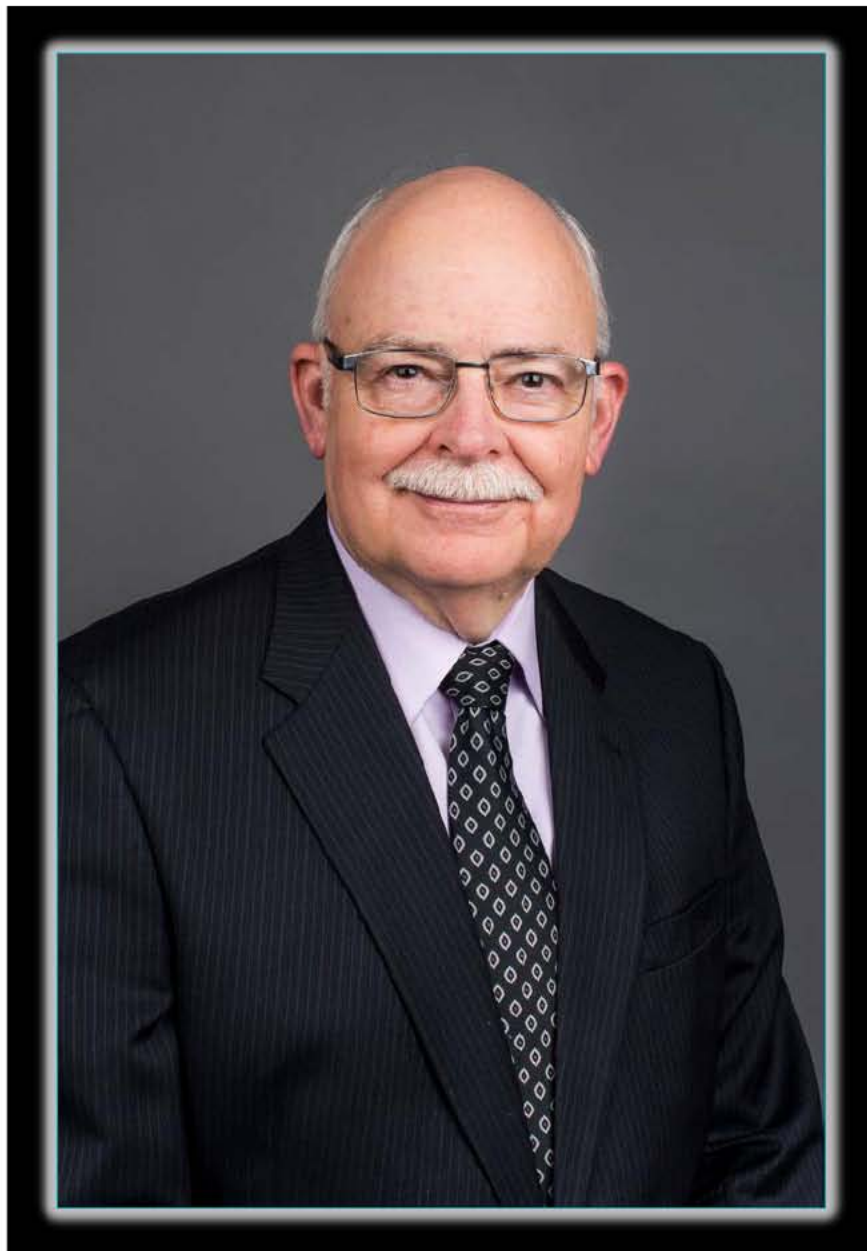
State Election and Cybersecurity Officials

North Dakota Secretary of State Organizational Chart

Updated June 2017



State Election and Cybersecurity Officials



Alvin (Al) Jaeger

NORTH DAKOTA SECRETARY OF STATE

IP Region 8 Team | North Dakota Election Background Package | August 18, 2017

State Election and Cybersecurity Officials

NASS Memberships: Election Committee, Election Cybersecurity Task Force

BIO Al Jaeger

Secretary of State Al Jaeger was elected North Dakota's fourteenth Secretary of State in 1992 and was reelected in 1996, 2000, 2004 (two year term), 2006, 2010, and 2014.

He serves on the North Dakota Emergency Commission, the Board of the North Dakota State Historical Society, and the North Dakota Board of University and School Lands.

Since becoming Secretary of State on January 1, 1993, Jaeger has been an active participant in the National Association of Secretaries of State (NASS). He has served nine terms on its Executive Committee. For 2015/2016, he was the Member-at-Large on the Executive Committee to the Notary Public Administrators' section of NASS. In July 2016, he was also appointed to his 21st consecutive term as Chairman of the NASS Standing Committee on Awards.

Jaeger was born in Beulah, ND in 1943. Raised in Beulah, he graduated from its high school in 1961. He attended Bismarck State College and in 1963 earned an Associate of Arts degree. In 1966, he received a Bachelor of Science degree from Dickinson State University majoring in Business Education with a minor in Speech. He also completed post-graduate work at the University of North Dakota in 1968 and Montana State University in 1970. Jaeger was chosen by the Bismarck State College National Alumni Association as the recipient of the 2009 BSC Alumnus of the Year Award. In 2011, he was named by Dickinson State University as an Alumni Fellow for the Department of Business and Management.

During his high school and college years, Jaeger worked for his father's excavating and ready-mix concrete company. He taught at Killdeer (ND) High School for three years (1966-1969) and for two years (1969-1971) at Kenmare (ND) High School. For two years (1971-1973), Jaeger worked as a marketing analyst in Fargo, ND, for the Mobil Oil Corporation. From 1973 to 1992, he was self-employed in Fargo as a real estate broker and owned his own real estate brokerage business.

He served in the North Dakota Army National Guard (1966-1972). Jaeger was an active member of Jaycee chapters in Killdeer, Kenmare, and Fargo where he was Secretary and Vice President. Before moving to Bismarck in 1993, he was an eighteen-year member of the Fargo Rough Riders Kiwanis Club where he served a term as President and several terms as club Secretary. Jaeger is a member of the Kiwanis Club of Bismarck and was its President for 2007-2008. He has been a Kiwanian for over 40 years. In Fargo, Jaeger belonged to Hope Lutheran Church and served a term as a council member, foundation board member, and for eighteen years as head usher. Now, a member of Charity Lutheran Church, Bismarck, he serves on several ministry teams.

Jaeger's wife, Kathy, died November 24, 2016. They have three adult children.

State Election and Cybersecurity Officials

Although not actively practicing, Jaeger maintains his North Dakota real estate broker's license and his membership in the Fargo-Moorhead Area Association of REALTORS and the North Dakota Association of REALTORS. He was an officer and a member of committees pertaining to education, professional standards, by-laws, and the Multiple Listing Service. Along with holding two professional REALTOR designations, he was named REALTOR of the Year in 1980 for the Fargo-Moorhead Area Association of Realtors (FMAAR) and was a nominee for North Dakota REALTOR of the Year. In 1997, FMAAR presented him with a Distinguished Service Award.

A long time blood donor, Jaeger attained the Gold Reward Level in November 2010 and has 111 donations as of May 2017.

<https://sos.nd.gov/secretary-state-bio>

State Election and Cybersecurity Officials



November 2003-present

North Dakota Deputy Secretary of State

Oct 1995 – Nov 2003

Camp of the Cross Ministries, Executive Director.

1983-1985

Attended Augsburg College – BA in Religion and Political Science

*Volunteers for Bridges of Hope in North Dakota as Advisory Board President. Bridges of Hope connects youth leaving the North Dakota Youth Correction Facility to mentors who offer an alternative environment to the one they were living in before being incarcerated.

Jim Silrum

NORTH DAKOTA DEPUTY SECRETARY OF STATE

IP Region 8 Team | North Dakota Election Background Package | August 20, 2017

State Election and Cybersecurity Officials



Doug Burgum
GOVERNOR, NORTH DAKOTA

IP Region 8 Team | North Dakota Election Background Package | August 20, 2017

State Election and Cybersecurity Officials

BIO

Doug Burgum took office as the 33rd governor of North Dakota on December 15, 2016. Doug brings a business leader's approach to diversifying the economy, creating 21st century jobs, and revitalizing our main streets.

Burgum's small-town upbringing and agricultural roots laid the foundation for his shared values of respect for the past, gratitude for the present and inspiration for the future.

Driven by a strong belief in North Dakota's people and a powerful dream, he returned to his home state and helped lead Great Plains Software from a small startup company in 1983 into an award-winning tech firm that employed thousands of team members from more than 220 cities across North Dakota.

Burgum led Great Plains as CEO through its initial public offering in 1997 and acquisition by Microsoft Corp. in 2001. He remained at Microsoft as senior vice president through 2007, helping the company stake a leading position in the global business applications software industry.

In 2006, Burgum reaffirmed his passion for North Dakota by founding Kilbourne Group, a real estate development firm committed to creating smart, healthy cities through vibrant downtowns. The company's substantial impact on revitalizing downtown Fargo inspired his Main Street Initiative.

In 2008, Burgum co-founded Arthur Ventures, a venture capital firm that invests in ambitious, mission-driven software companies. The success of those people and businesses guided by Burgum's leadership and inspiration has created billions of dollars of shareholder wealth and thousands of jobs. In 2009, then-Gov. John Hoeven awarded Burgum the [Theodore Roosevelt Rough Rider Award](#), North Dakota's highest citizen honor. The award recognized Burgum for his business leadership and numerous philanthropic efforts, including the Doug Burgum Family Fund, which focuses its charitable giving on youth and education.

Born August 1, 1956, Burgum grew up in Arthur, N.D. He has maintained his commitment and connection to his roots through family farm partnerships, by serving as a member for Arthur Companies, Inc., a diversified agribusiness company founded by his grandparents in 1906, and through a ranching partnership in the Badlands of western North Dakota. Burgum graduated with a bachelor's degree in university studies from North Dakota State University in 1978. He earned a master's of business administration from the Stanford University Graduate School of Business in 1980.

He was elected governor on Nov. 8, 2016, in his first run for political office.

Burgum is married to Kathryn Helgaas Burgum and has two sons, Joe and Tom, and a daughter, Jesse.

Elections Infrastructure Information

Counties: 53

Number of Polling Locations: 259; 45 of 53 counties have less than 10 polling locations within the county with the average for the 53 counties of between 2-3 polling locations

Voter Registration: Not required

Rationale: North Dakota is a rural state and its communities maintain close ties and networks. North Dakota's system of voting, and lack of voter registration, is rooted in its rural character by providing small precincts. Establishing relatively small precincts is intended to ensure that election boards know the voters who come to the polling places to vote on Election Day and can easily detect those who should not be voting in the precinct.

Q: What voting equipment will voters use to cast their ballots?

- A voter uses a paper ballot that is inserted into a scanner after the voter casts his or her ballot.

2015-2017 North Dakota Election Laws - Excerpts

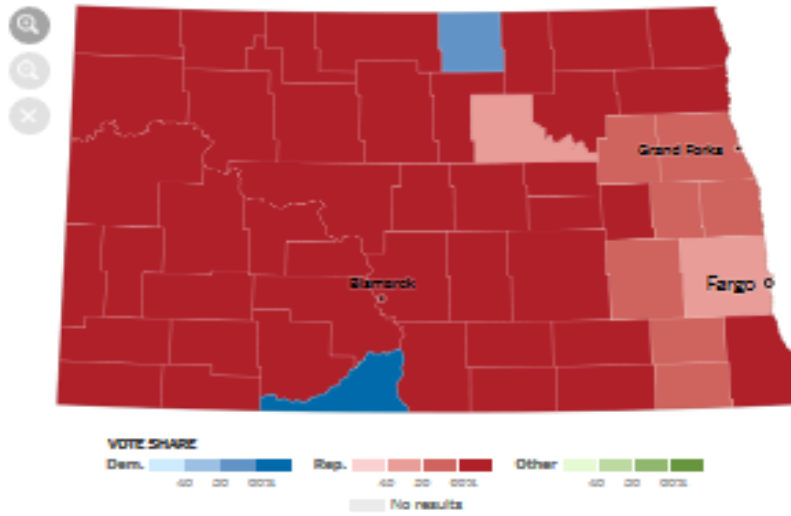
16.1-06-10.1. Electronic counting machines authorized -- Sharing of machines.

The use of electronic counting machines is authorized in any election precinct upon finding and declaration by resolution of the city governing body, and also of the board of county commissioners of the county in which the election precinct is located, that the use is advisable or necessary in that precinct. Thereafter, electronic counting machines may be procured, on a temporary or permanent basis, under terms and conditions, including assumption and division of cost of acquisition and maintenance by the city and county, agreed upon by the respective governing bodies, provided the machines being procured have been certified for procurement and use in the state by the secretary of state according to section 16.1-06-26. Two or more counties may enter an agreement concerning the shared use and transport between counties of electronic counting machines and apportioning of expenses. Any electronic counting machine used in an election must be so constructed that when properly operated it registers or records correctly and accurately every vote cast.

16.1-06-26. Secretary of state to adopt rules for the purpose of certifying and decertifying electronic voting systems and electronic counting machines.

The secretary of state may adopt rules according to subsection 3 of section 16.1-01-01 for certifying and decertifying electronic counting machines authorized in section 16.1-06-10.1 and electronic voting systems authorized in section 16.1-06-11, including any software, hardware, and firmware components used as a part of an electronic voting system or electronic counting machine for use and procurement in the state.

Elections Infrastructure Information



Vote by county	Trump	Clinton
Cass	29,916	21,361
Burleigh	22,522	10,661
Grand Forks	16,340	10,661
Ward	16,626	5,908
Morton	11,326	2,060
Williams	10,069	1,725
Stark	9,755	1,752
Stutsman	6,719	2,456
Richland	4,787	2,064
Barnes	2,180	1,527

[+ Show all counties](#)

Elections Infrastructure Information

U.S. Election Assistance Commission



NORTH DAKOTA

State Participation: **Requires Federal Certification.** ND requires that its voting systems are tested by an EAC accredited independent testing authority as fulfilling the requirements of the EAC voluntary voting system guidelines.

Applicable Statute(s): “The secretary of state may adopt rules according to subsection 3 of section 16.1-01-01 for certifying and decertifying electronic counting machines authorized in section 16.1-06-10.1 and electronic voting systems authorized in section 16.1-06-11, including any software, hardware, and firmware components used as a part of an electronic voting system or electronic counting machine for use and procurement in the state.” [N.D. CENT. CODE § 16.1-06-26](#) (2008).

Applicable Regulation(s): “Prior to procurement and subsequent use in this state, a company supplying electronic voting systems shall give written notice to the secretary of state and provide a demonstration certifying that its system complies with applicable laws and is certified by a voting system test laboratory accredited by the EAC. If the secretary of state approves the voting system, the secretary of state shall issue a certificate of approval. Any substantive changes or modifications in electronic voting systems may be certified by the secretary of state with or without the demonstration described in this section for initial approval provided that the modified system has been certified by a voting system test laboratory accredited by the EAC.” [N.D. ADMIN. CODE 72-06-01-02](#) (2009).

State Certification Process: A company supplying electronic voting systems will given written notice to the Secretary of State and provide a demonstration certifying that the voting systems comply with applicable laws and is certified by an independent testing authority accredited by the EAC as fulfilling the requirements of the EAC voluntary voting system guidelines. If the Secretary of State approves the voting system, the Secretary of State shall issue a certificate of approval. [N.D. ADMIN. CODE 72-06-01-02](#) (2009).

Fielded Voting Systems: *[After the EAC completes and issues the 2008 Election Administration and Voting Survey, information about fielded voting systems will be added to this document. In the meantime, readers may find information on the voting systems at the following website (if available)].*
<http://www.nd.gov/sos/elect/vote/>

2018 Elections Information

Primary Election: June 12, 2018

General Election: November 6, 2018

Section 5 – Federal, State, and County Offices on Ballots in 2018

CONGRESSIONAL

United States Senator6 year term
 Representative in Congress2 year term

Incumbents
Heidi Heitkamp (D)
Kevin Cramer (R)

STATE

Statewide Political Party Ballot

Secretary of State4 year term
 Attorney General4 year term
 Agriculture Commissioner4 year term
 Tax Commissioner4 year term
 Public Service Commissioner6 year term

State Legislative District Seats

24 seats Senate (all odd numbered districts)4 year term
 48 seats House of Representatives (all odd numbered districts)4 year term

No-Party Ballot

Justice of the Supreme Court (statewide)10 year term
 Judges of the District Court6 year terms (exceptions noted below)

<u>Judicial District</u>	<u>Judgeship Number(s)</u>
East Central	8
Northwest	5 and 6 (term ends 12/31/2022 for both)
North Central	3 and 4
Northeast	3 (term ends 12/31/2020)
Northeast Central	1, 2, and 4 (term ends 12/31/20 for judgeship 4 and 12/31/2022 for judgeship 1)
South Central	3, 4, and 9 (term ends 12/31/2022 for judgeship 9)
Southeast	3
Southwest	1, 3, and 4 (term ends 12/31/2022 for judgeship 4)

COUNTY (Depending on county structure)

County Commissioners4 year term

Director, Southwest Water Authority (June Election only)4 year term
 Bowman, Golden Valley, Hettinger, Mercer, Morton (one position outside Mandan city limits and one within the city of Mandan), Stark (one position outside Dickinson city limits and one within the city of Dickinson), each jurisdiction elects one director.

Supervisor, Soil Conservation District (November Election only)6 year term

Director, Garrison Diversion Conservancy District4 year term
 Benson, Cass, McHenry, McLean, Pierce, Ramsey, Renville, Richland, Stutsman, Traill, Ward, and Wells

Some counties will vote on:

- A continuation of a \$1 per line per month fee on telephone service for the costs associated with E-911 service. [NDCC § 57-40.6-02](#)

Nevada

State Election and Cybersecurity Officials



BARBARA CEGAVSKE
SECRETARY OF STATE, NEVADA

BIO

Barbara Cegavske was elected as Nevada Secretary of State in 2014 and assumed office on January 5, 2015. With more than 33 years of combined public service and small business experience, Cegavske brings a unique blend of business acumen and legislative expertise to the Secretary of State's office.

Cegavske entered public service in 1996 when she was elected to serve in the Nevada Assembly representing Clark County District 5 for three consecutive terms. In 2002, Cegavske ran for and successfully won a state Senate seat for Clark County District 8. She served three full terms before assuming the role of Secretary of State.

During her time in the Nevada Legislature, Cegavske assumed leadership roles as Co-Assembly Assistant Minority Floor Leader, Assistant Assembly Minority Whip, Senate Minority Whip, and Senate Assistant Minority Leader. She also chaired the Senate Committee on Legislative Operations and Elections for three legislative sessions and was vice-chair of the Senate Committees on Human Resources and Education; Human Resources and Facilities; and Legislative Affairs and Operations. In all, Cegavske served in nine regular sessions and 13 special sessions of the Nevada Legislature.

As a daughter of small business owners, Cegavske rolled up her sleeves and pitched in with her siblings after school and during summer vacations to help the family business. Her introduction to the free-market system proved to be valuable first-hand knowledge when she and her husband Tim became owners of a 7-Eleven franchise. Over the course of 13 year, the Cegavske faces daily challenges but also experienced the rewards of employing fellow Nevadans and contributing to the state's economy.

State Election and Cybersecurity Officials

They also learned about onerous regulations that placed burdens on their business and disincentives for a business to be able to grow and thrive.

Born and raised in Minnesota, Cegavske has been a proud Nevadan for the past 40 years. She has two sons, Adam and Bret, who graduated from UNR and UNLV respectively and are raising their own families in Las Vegas. Cegavske and her husband are the proud grandparents of five grandchildren.

State Election and Cybersecurity Officials

State Election and Cybersecurity Officials



CALEB CAGE
CHIEF OF THE DIVISION OF EMERGENCY MANAGEMENT
AND
HOMELAND SECURITY ADVISOR, NEVADA
BIO

Caleb S. Cage was appointed as Chief of the Division of Emergency Management and Homeland Security Advisor on July 6, 2015. He is a graduate of the United States Military Academy, West Point, where, upon graduation in 2002, he was commissioned as a Field Artillery officer and was assigned to the 1st Infantry Division in Bamberg, Germany. During this period, he served as a company executive officer and later as a motorized rifle platoon leader in the city of Baqubah, Iraq.

Caleb's military career spanned five years and various positions, including Fire Direction Officer, Executive Officer, and Battery Commander. He also served a second yearlong tour in Iraq in 2006 as a Corps Information Operations battle captain in the Corps Joint Operations Center in Baghdad.

Upon separating from the Army, Cage began his civilian career as a Senior Policy Advisor to the Lieutenant Governor, where he developed and managed several successful outreach initiatives aimed at serving Nevada's veterans. In 2010, he was appointed to serve as Executive Director of the Nevada

Office of Veterans Services (NOVS), a cabinet-level agency responsible for serving veterans through two state veteran cemeteries, a comprehensive veterans service officer program, and 180-bed long term care skilled nursing facility.

In addition to these efforts, Cage also established Nevada's Green Zone Initiative, an effort to improve outcomes for veterans through policy development, service provider coordination, and outreach.

Because of the success of his work in these areas, Cage was asked to move into the position of Director of Military and Veterans Policy, a newly-created position in the Office of Governor Brian Sandoval in August of 2013.

State Election and Cybersecurity Officials



BRIAN SANDOVAL GOVERNOR, NEVADA

BIO

Republican Nevada Governor Brian Sandoval is the first Hispanic to hold statewide office, as well as the youngest chairman of the Nevada Gaming Commission.

Brian Sandoval was born on August 5, 1963, in Redding, California. Of Latino ancestry and Mexican roots, he became the first Hispanic in Nevada to hold statewide office. Sandoval served on the Nevada Assembly and its Gaming Commission. He then served as a United States District Court judge and the Nevada attorney general before he went on to become the state's governor in 2010.

He earned his bachelor's degree in English and economics in 1986 from the University of Nevada and then earned a law degree from the Ohio State University Moritz College of Law in 1989. He opened his own law form in Reno a decade later.

Prior to opening his own law form, Sandoval ran for a seat on the Nevada Assembly in 1994. He won the seat and won re-election in 1996, but resigned two years later, when then-Governor Bob Miller appointed him to serve as a member of the Nevada Gaming Commission, which oversees the state's gaming industry. The next year, in 1999, Sandoval became chairman of the commission: At age 35, he was the youngest person ever to serve as chairman of the commission. During his time on the commission, Sandoval fought national efforts to block gaming on college sports events, among other efforts.

State Election and Cybersecurity Officials

Sandoval ran for the Nevada Attorney General seat in November 2002. He won the election, defeating Democrat challenger John Hunt, and took office in January 2003. While in office, Sandoval sponsored legislation strengthening Nevada's laws against drug abuse, domestic violence and human trafficking. He also developed the state's first Public Integrity Unit.

In 2004, Democratic U.S. Senator Harry Reid recommended to then-President George W. Bush that Sandoval be nominated for the United States District Court for the District of Nevada. By the fall of 2005, the U.S. Senate unanimously confirmed Sandoval (89-0, with 11 senators not voting), who then received his judicial commission. Sandoval resigned from that position on September 15, 2009 – the same day he announced that he was running for the governorship of Nevada.

Sandoval won the 2010 gubernatorial election, in which he faced challenger Democratic Rory Reid, chair of the Clark County Commission and son of U.S. Senate Majority Leader Harry Reid. Sandoval won every county in the state with a majority, with the exception of Clark County. The election victory made Sandoval the first Hispanic candidate elected to statewide office in Nevada.

In 2012, Sandoval was rumored to be on Republican presidential candidate Mitt Romney's list of vice-presidential possibilities. In June 2012, *CNN* published an article taking a close look at how Romney could court the Latino vote. In addition to studying the possibility of Romney choosing New Mexico Governor Susana Martinez, *CNN* examined Sandoval's chances. "Sandoval is a budget-cutting, government-shrinking Republican," *CNN* wrote, "but he favors abortion rights, which could be a drawback as GOP running mate. And though he's Latino, he doesn't speak Spanish."

But Sandoval said he would not want to be considered as a vice-presidential nominee, stating that he had "the best job in the country," according to the *Las Vegas Sun*. In its own explanation of why Sandoval wasn't really in the running, the *Las Vegas Sun* wrote, "First is that he's simply not charismatic and would have an incredibly hard time commanding respect, not to mention being totally unable to sell a warped ideological agenda to America." The April 2012 article went on to say that Sandoval would do more harm than good, if he were ever elected as vice president.

Despite rumors regarding Sandoval's potential vice-presidential nomination, Romney announced U.S. Republican Congressman Paul Ryan as his running mate for vice president in August 2012.

Sandoval is married to Kathleen Sandoval, a native Nevadan, and together they have three children.

Election Infrastructure Information

Counties: 16

Voter Registration/Qualifications: Criteria to be eligible to vote in Nevada includes: must be a Citizen of the United States; must be a Nevada at least 30 days before the date of an election; must be a resident of your precinct for at least 10 days before the election; be at least 18 years old on or before the date of the election; not have been declared mentally incompetent by a court of law; and not claim any other places as your legal residence. Voters can register online, in person or through the mail.

Persons with convictions of a non-violent felony will have their voting rights restored after discharge from incarceration and/or parole. Persons convicted of a violent felony, or a second felony, will need to apply to have civil rights restored.

Voter Equipment used to cast ballots: Computers at each polling site connect to the Election Department's centralized voter registration files. Voter records are updated at the time of voting, thus preventing anyone from voting twice. To begin the voting process, voters provide their name to the Computer Clerk and he/she will verify identity and eligibility to vote, then issue a voting machine activation card. The voter then proceeds to a touch-screen voting machine to vote; inserts the card into the machine to activate it for their specific precinct. When voting is finished, the card is immediately returned to an election official. Nevada, particularly Clark County Election Department is recognized throughout the United States as a leader in incorporating technology into the voting process.

Touch-screen machines are used in all Clark County polling locations. Similar in appearance to an ATM machine, the machines make voting easy and assists voters throughout the voting process. Choices are registered and ballots cast electronically by touching a screen. When all selections are made, a printer records the choices and the voter confirm they are accurate before the ballot is cast. If an error is made, the paper record is voided by the voter and mistakes are corrected on the touch-screen machine. The printer reprints the new selections. After the printout is confirmed as accurate, the voter casts their ballot. The paper record then scrolls out of view and the machine resets for the next voter. Clark County also began using optical scan voting systems for the first time in the 2004 elections. Voters receive voting instructions when they receive their optical scan paper ballot.

Accuracy and Integrity/Storage:

The electronic touch-screen voting machines are stand-alone units and cannot be "hacked into" because they are not on a network. The software used on each machine is obtained directly from the Secretary of State who received it directly from the federal laboratory that tested it. It is then verified with hash coding algorithms to ensure no one has tampered with it and that it is the exact software the federal laboratory tested. The machines are stored in a secure environment in which access is limited and monitored by cameras, motion sensors, and various other sensor and personnel monitoring systems. The machines are delivered to the polling locations in a manner that prevents anyone from tampering with them without it being immediately evident to election poll workers. Finally, when the election is over, all results are audited. The number of individuals who signed precinct registers are matched with the number of ballots cast, and the electronically recorded results are matched with the results verified by the voters on the paper printouts.

Election Infrastructure Information

Nevada Revised Statutes (NRS) (Voting Equipment Requirements) Chapters 293, 293B, 293C, 293D, 294A, 295, 298, 304 and 306

The links on this page will take you to the [Nevada Legislature](#) Website.

REQUIREMENTS

NRS 293B.063 System to meet or exceed standards established by Federal Election Commission pursuant to federal law. No mechanical voting system may be used in this State unless it meets or exceeds the standards for voting systems established by the Federal Election Commission pursuant to federal law.

(Added to NRS by [1993, 2199](#); A [2003, 2186](#); [2005, 1438](#))

NRS 293B.065 Privacy and independence. A mechanical voting system must secure to the voter privacy and independence in the act of voting.

(Added to NRS by [1975, 1523](#); A [1985, 1099](#); [2003, 2187](#))

NRS 293B.070 Full choice of candidates and measures. A mechanical voting system must provide facilities for voting for the candidates of as many political parties or organizations as may make nominations, and for or against measures.

(Added to NRS by [1975, 1523](#); A [1985, 1099](#))

NRS 293B.075 Full choice of candidates for offices; vote against all candidates. A mechanical voting system must permit the voter to vote for any person for any office for which he or she has the right to vote, but none other, or indicate a vote against all candidates.

(Added to NRS by [1975, 1523](#); A [1985, 1099](#))

NRS 293B.080 “Straight” or “split” ticket. A mechanical voting system must, except at primary elections, permit the voter to vote for all the candidates of one party or in part for the candidates of one party and in part for the candidates of one or more other parties.

(Added to NRS by [1975, 1523](#); A [1985, 1099](#); [1995, 2632](#))

NRS 293B.082 Record of votes cast; record printed on paper. Each mechanical voting system must provide a record of the votes cast on that system. The record must be printed on paper.

(Added to NRS by [1995, 2785](#))

NRS 293B.084 Required features and design of mechanical recording device which directly records votes electronically; availability and use of paper record for manual audit.

1. A mechanical recording device which directly records votes electronically must:

(a) Bear a number which identifies that mechanical recording device.

(b) Be equipped with a storage device which:

(1) Stores the ballots voted on the mechanical recording device;

(2) Can be removed from the mechanical recording device for the purpose of transporting the ballots stored therein to a central counting place; and

(3) Bears the same number as the mechanical recording device.

(c) Be designed in such a manner that voted ballots may be stored within the mechanical recording device and the storage device required pursuant to paragraph (b) at the same time.

(d) Be capable of providing a record printed on paper of:

(1) Each ballot voted on the mechanical recording device; and
(2) The total number of votes recorded on the mechanical recording device for each candidate and for or against each measure.

2. The paper record described in paragraph (d) of subsection 1 must be printed and made available for a manual audit, as necessary.

(Added to NRS by [1995, 2786](#); A [2003, 1657, 2187, 3516](#); [2007, 2605](#))

NRS 293B.085 Several elective to same offices; effect of overvote. A mechanical voting system must permit the voter to vote for as many persons for an office as the voter is lawfully entitled to vote for, but no more. If a voter casts more votes for an office than the voter is lawfully entitled, the counting device or electronic computer must be programmed so that those votes are not counted. The remainder of the voter's ballot must be counted if it is otherwise lawfully voted.

(Added to NRS by [1975, 1523](#); A [1985, 1099](#))

NRS 293B.090 Prevention of voting more than once. A mechanical voting system must prevent the voter from voting for the same person more than once for the same office.

(Added to NRS by [1975, 1523](#); A [1985, 1100](#))

NRS 293B.095 Measures on which voter is entitled to vote. A mechanical voting system must permit the voter to vote for or against any measure the voter may have the right to vote on, but none other.

(Added to NRS by [1975, 1523](#); A [1985, 1100](#))

NRS 293B.100 Correct registration or recording of votes. A mechanical recording device must correctly register or record, on the voter's ballot, all votes cast for any and all persons and for or against any and all measures.

(Added to NRS by [1975, 1523](#); A [1985, 1100](#))

NRS 293B.103 Voting receipts. If a mechanical voting system is used whereby votes are directly recorded electronically, a voting receipt may be used.

(Added to NRS by [1983, 1289](#); A [1985, 1100](#); [1995, 2787](#); [2007, 1167, 2606](#))

Election Information

Upcoming Elections

2018 November 6 Election : 2018 November 6 General Election

Deadlines

- October 6, 2018 **Voter Registration Ends:**Last day to register to vote or to update your existing registration, without having to appear in-person at the Election Department offices, or without having to or register on the Secretary of State's website.
- October 20, 2018 **Early Voting/In Person Absentee voting starts:**Any voter registered in Clark County may vote at any early voting site within the County. Hours and days vary by location.
- October 30, 2018 **Absentee Ballot Request deadline - By Mail:**Last day for the Election Department to RECEIVE WRITTEN mail ballot requests.
- November 2, 2018 **Early Voting/In Person Absentee voting ends:**Any voter registered in Clark County may vote at any early voting site within the County. Hours and days vary by location.
-

Open Source ND Media Coverage

How states are handling Trump's voter information request

- By The Associated Press
- Aug 9, 2017.

These are state-by-state responses to a request for detailed voter data from President Donald Trump's Presidential Advisory Commission on Election Integrity, which is investigating voter fraud. The information indicates whether a state is willing to comply with, is denying or is undecided on the request for data. Some of the states that are willing to comply have fees or other requirements of the commission. All states that have agreed to provide the information are withholding some details that the commission said it wanted only if it was considered public under state law. The commission sent one request in late June and another in July after a court said the data collection could move ahead.

NEVADA

Comply

Republican Secretary of State Barbara Cegavske says her office has not changed its position in the wake of the renewed commission request. It will provide public information but not data kept confidential under state law such as Social Security numbers or how people voted. The state will turn over voter names, addresses, telephone numbers, dates of birth, party affiliation and turnout.

04/18/2017 04:18 pm ET Updated Apr 19, 2017

Nevada Secretary Of State Says She Has Evidence Of Voter Fraud In Presidential Election

[Like President Donald Trump, Secretary of State Barbara Cegavske produced no evidence](#)

By Sam Levine

The Nevada secretary of state has accused her state's Department of Motor Vehicles of facilitating voter fraud and said she has evidence non-citizens voted in last year's presidential election. Secretary of State Barbara Cegavske (R) wrote in a letter Friday to DMV Director Terri Albertson that DMV workers had been accepting voting applications from non-citizens and forwarding them to the secretary of state's office. Cegavske said she had evidence non-citizens voted in the presidential election, but didn't elaborate.

President Donald Trump has stoked fears of voter fraud, claiming repeatedly that millions illegally voted in the 2016 election. Like Cegavske, Trump has offered no evidence, but the White House is gearing up for a federal investigation. Voting fraud is extremely rare.

Open Source ND Media Coverage

Cegavske, who supports requiring voters to produce a photo ID, said in January that while there was no evidence of voter fraud in the state during the presidential election, she said she was aware of attempted fraud related to registration. It's unclear what changed.

"There's nothing else," Gail Anderson, Cegavske's deputy for southern Nevada, told the Nevada Independent, referring to the secretary of state's letter alleging voter fraud. "When we have information that can be provided, we certainly would do that." Cegavske's office did not respond to repeated requests for comment.

Gov. Brian Sandoval (R) seemed unaware of the evidence for Cegavske's claim, but said Monday he "expects to hear more." Joe Gloria, registrar of voters in Clark County, the most populous in Nevada, told the Independent he was unaware of any voter fraud probe. Federal law requires states to allow residents to register to vote at DMV offices.

The Nevada DMV director responded to Cegavske's allegation with a strongly worded letter on Saturday that said the secretary of state's office had signed off on the DMV's voter registration procedures. "Your letter comes as a complete surprise as you and your office have reviewed, contributed to, and approved the processes you are expressing concerns about," DMV director Albertson wrote. Albertson noted that DMV officials would flag suspect applications for further review by a county clerk or registrar to determine voting eligibility.

The governor defended the DMV in the public dispute. "They were operating under the policies and guidelines that were adopted pursuant to input, review and approval of the Nevada Secretary of State's Office," Sandoval told the Independent. "I'm going to rely on (DMV Director) Terri Albertson — they are proceeding in accordance with what has been approved," Sandoval told the Las Vegas Review-Journal. "So I guess the ball is in the secretary of state's court." The ACLU of Nevada said in a statement on Monday that election officials, not the DMV, had the burden of verifying the eligibility of voters.

Under the National Voter Registration Act, the DMV "cannot make determinations regarding voter eligibility" and must send voter registration applications to state election officials for a judgment, the ACLU said.

FOR OFFICIAL USE ONLY

ELECTION CRITICAL INFRASTRUCTURE WORKING GROUP MEETING

DATE: Thursday September 14, 2017
TIME: 8:30 a.m. – 3:00 p.m.
LOCATION: 1335 East West Highway, Suite 4300
Silver Spring, MD 20910

BOTTOM LINE UP FRONT (BLUF)

- This is the third meeting of the Election Critical Infrastructure Working Group (ECIWG), which is the precursor to the Election Infrastructure (EI) Subsector GCC.
- ECIWG members have provided feedback on the draft GCC charter that was updated based on discussion at the August 21 meeting in Anaheim.

OBJECTIVES/DESIRED OUTCOME OF MEETING:

- ECIWG should reach consensus on final GCC membership composition.
- ECIWG should reach consensus on final GCC Charter language.
- ECIWG should discuss MS-ISAC potential to be used as the EI Subsector ISAC.

BACKGROUND:

- This is expected to be the final ECIWG meeting before the first official meeting of the EI GCC, tentatively scheduled for mid-October 2017. The primary goal of this meeting is to finalize organizational details so the GCC can approve the charter at its first meeting.
- NPPD has co-chaired meetings of this group in Albany, NY on July 25-26 and Anaheim, CA on August 21 to discuss the formation of an Election Infrastructure Subsector GCC.
- DHS/I&A has contacted the senior election officials in each state, territory, and the District of Columbia to begin the process to obtain Secret-level clearances to facilitate the passing of classified information related to election infrastructure.
- DHS/OGC has committed to provide training for ECIWG members on how to respond to FOIA requests.
- The National Association of Secretaries of State (NASS) raised minor concerns with some of the terminology in the draft GCC charter. Expect this to be brought up in the meeting. Charter will need to be defended as written or amended to appease the respective commenting organizations.

PARTICIPANTS:

- See Attachment C – ECWG VIP Bios.

PRESS PLAN:

- Closed to press.

FOR OFFICIAL USE ONLY

Page 1 of 3

FOR OFFICIAL USE ONLY

ATTACHMENTS:

- A. ECIWG Meeting Agenda_DRAFT_9.07.17
- B. Draft EI GCC Charter, 7 Sep
- C. ECIWG VIP Bios

Prepared by: (b) (6) EI SSA Team Lead (b) (6) 33
(b) (6) Program Analyst, (b) (6)
(b) (6)

FOR OFFICIAL USE ONLY

TALKING POINTS

- Thank the ECIWG members for their continued participation in the standup of the Election Infrastructure GCC.
- Thank the Election Assistance Commission for hosting today's meeting.
- Express DHS appreciation of the participants' continued engagement in constructive dialog as all sides work together to build a mutually beneficial subsector partnership structure.
- Note that the meeting's goal is to reach consensus on the GCC membership construction and proposed charter so it can be formally adopted by the GCC at its first meeting, tentatively scheduled for mid-October.
- Note that the group should to begin to outline its collective EI strategic objectives as it moves toward developing the agenda for the first formal GCC meeting.
- Encourage the members to speak up during the discussion, acknowledging the importance of continuing the good participation from the previous meetings.
- Turn the floor over to the facilitator to begin moving through the agenda.

FOR OFFICIAL USE ONLY

Page 3 of 3

Judd Choate
President, National Association of State Election Directors (NASED)
Director, Division of Elections, Colorado Department of State

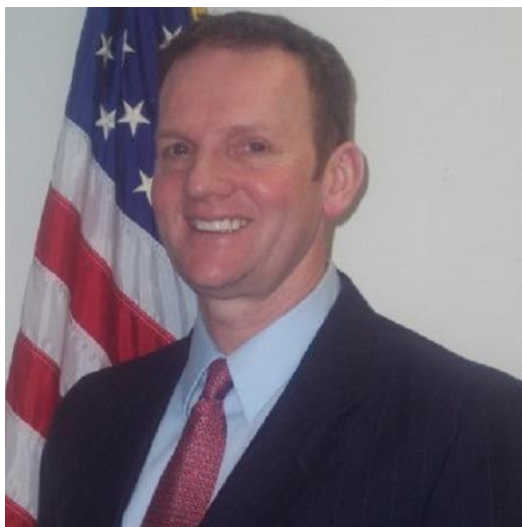


Dr. Judd Choate is the state elections director for Colorado. Prior to joining the Colorado Department of State in 2009, Judd practiced election law at the Denver firm of Kelly Garnsey Hubbell & Lass. He also served as a law clerk for Colorado Supreme Court Justice Alex J. Martinez and as a summer clerk for Judge Timothy Tymkovich of the 10th Circuit Court of Appeals.

For several years prior to law school, Judd was a professor of political science at the University of Nebraska, where he taught courses on campaigns and elections. Judd is the author of a book and several peer-reviewed articles on political behavior.

Judd is the 2017 president of the National Association of State Election Directors. He has a J.D. from the University of Colorado Law School and both a Ph.D. and M.A. in political science from Purdue University.

Bob Giles
President-elect, NASED
Director, New Jersey Division of Elections



Robert Giles was appointed to the position of Director of the New Jersey Division of Elections on May 1, 2008. Prior to this, he was employed by the Ocean County Board of Elections beginning in 1995 working as an investigator, a voting machine technician, an assistant supervisor and supervisor. He is an Adjunct Professor for Rutgers University's Center for Government Services teaching Election Administration.

Robert is currently a member of the Standards Board for the United States Election Assistance Commission. He is also serving as the Standards Board representative on the Technical Guidelines Development Committee which is responsible for developing the next set of federal standards for voting equipment. He is currently a member of the Council of State Governments Election Technology Working Group. He served as a member of the Department of Homeland Security's Cyber Unified Coordination Group for the 2016 Presidential Election. He is the President Elect for the National Association of State Election Directors and served as Vice President of the New Jersey Association of Election Officials and was a member of its Legal and Legislative Committee.

Robert graduated from Denison University, Granville, Ohio in 1986.

Connie Lawson
President, National Association of Secretaries of State (NASS)
Secretary of State, Indiana



Connie Lawson is Indiana's 61st Secretary of State. As Indiana's Chief Elections Officer, she is focused on ensuring the integrity and security for our state's elections. Since taking office, Secretary Lawson has championed sweeping election reforms and has led the effort to clean Indiana's voter rolls. A tireless advocate for increasing Indiana's financial literacy and protecting Indiana investors, Secretary Lawson educates Hoosiers about smart money decisions and fights for stringent penalties for white collar criminals. Secretary Lawson is directing substantial innovation and leveraging cutting edge technology to improve how businesses interact with government through INBiz, the state's one-stop business portal.

Secretary Lawson lends her experience to help many great organizations. She is President of the National Association of Secretaries of State, an honorary governor of the Richard G. Lugar Excellence in Public Service Series, the honorary chairwoman of the Lupus Foundation of Indiana, and a co-chair of the Hendricks County United Way. In 2017, President Donald Trump appointed her to serve as a member of the Advisory Commission on Election Integrity.

Prior to serving as Secretary of State, Lawson served in the Indiana Senate for sixteen years, where she quickly earned the admiration of her colleagues and made history in 2006 when she was selected as the first woman to serve as Majority Floor Leader. Before joining the Indiana Senate, Lawson served as Clerk of the Hendricks County Circuit Court.

She and her husband Jack own Lawson & Company, an auctioneer and real estate company. Lawson is a life-long Hoosier and resident of Hendricks County.

Jim Condos
President Elect, National Association of Secretaries of State (NASS)
Secretary of State, Vermont



Jim Condos is Vermont’s 38th Secretary of State. First elected in 2010, he has an extensive background in business as well as both municipal and local government. Jim has one daughter, Chelsea. Although born in Orange, NJ, in 1951, Jim moved to Burlington with his family when he was four years old. He later moved to South Burlington and graduated from South Burlington high school and then the University of Vermont.

With over 30 years of business experience gained working in a variety of diverse companies—from a global Fortune 100, to a Vermont-based, family-owned, grocery distribution company, to a Vermont regulated utility—Jim understands Vermont business needs. “In government, as in business, I focus on the customer experience. If there is anything that I learned in my thirty plus years working in the business sector, it is that information and accessibility are key.”

Initially, getting involved in local government to help solve a local zoning issue, Jim began reading up on statute and involving himself in municipal government and has been an avid advocate for the people’s right to know ever since. Jim served for 18 years (1989 to 2007) on the South Burlington City Council, the last eight years of which he served as chair.

In 2001, Jim was elected as a Senator for Chittenden County. He served four terms and chaired three integral committees: Education (2003–2004); Government Operations (2005–2006); Joint Legislative IT (2008).

Since his election as Secretary of State in 2010, Jim has worked tirelessly to bring greater transparency to all levels of government. During each non-election year, Jim tours the state on his “Transparency Tour” discussing open meeting and public records laws with local officials and the public. While the official tour is biennial, he will gladly bring his presentation to any town that requests it, at all times of the year.



Talking Points

- Thank the Nordic Innovation Labs representatives for their interest in meeting and for their efforts to advance the security and resilience of the Nation's election infrastructure.
 - Acknowledge your awareness of their participation in setting up the DEF CON Voting Machine Hacking Village.
- Express DHS/CS&C's interest in working with Nordic Innovation Labs to become more involved in regular testing and evaluation of election systems to provide value and better protect the Election Infrastructure Subsector.
 - Typically, when DHS engages in the kind of testing that occurred at DEF CON, it prefers to do so behind closed doors.
 - This provides an opportunity to work with vendors to identify and mitigate vulnerabilities before bringing them to light publicly. This protects both the individual vendor and the sector.
- Discuss the designation of Election Infrastructure (EI) as a critical infrastructure subsector of the Government Facilities Sector in 2017.
 - This Administration supports this designation and DHS will not change the designation of Election Infrastructure as a subsector.
- Typically, under the critical infrastructure subsector designation, partners organize for their collective good and receive prioritized assistance from the Federal government for their efforts to manage risks to the sector or subsector.
 - Participation in the election infrastructure subsector is entirely voluntary.
 - The sector structure is a tool to help facilitate timely, coordinated information sharing between Federal government and partners, in State, Local, Tribal and Territorial government and the private sector.
 - For each sector or subsector, there is a designated Federal government Sector-Specific Agency (SSA), which serves as the Federal interface for coordination of activities related to critical infrastructure security and resilience.
 - The National Protection and Programs Directorate's (NPPD) Office of Infrastructure Protection will execute the SSA responsibilities for the Election Infrastructure Subsector.
 - Sectors and subsectors establish a governance structure based on coordinating councils.

**8th Annual Billington Cybersecurity Summit
September 13, 2017**

Agenda

“Ensuring Cybersecurity In Unprecedented Times”

7:00 – 8:00 am Registration, Continental Breakfast, and Networking

7:55 – 8:00 am Opening Remarks

- (b) (6), Chair, 8th Annual Billington CyberSecurity Summit

8:00 – 8:20 am Opening Keynote

- The (b) (6) of National Intelligence

8:20 – 8:50 am The Cybersecurity Threat Landscape—From Ransomware to Russia

From Petya to WannaCry to alleged nation state interference into the U.S. elections, cybersecurity is front and center in the mindset of government, industry, the military, and policymakers. This cross-section of distinguished experts, including the recently retired Deputy Director of the National Security Agency, will address from an insider’s viewpoint the state of cybersecurity. Key critical infrastructure in the private sector, the security of critical data, and sensitive military and intelligence information, as well as financial and healthcare information, are all at stake.

- What are the motives in the attacks by key nation states, in particular China and Russia?
- What is fact and what is fiction?

Moderator:

- (b) (6), Vice President and Ambassador at Large, Cylance

Speakers:

- (b) (6), National Security Agency
- (b) (6), Booz Allen Hamilton
(Former Director, NSA and Former DNI)
- Christopher Krebs, Senior Official Performing the Duties of the Under Secretary, NPPD, DHS
- (b) (6) Emerging Security Challenges, NATO

8:50 – 9:30 am Top Cybersecurity Priorities for CISOs in FY18—Implementing the Executive Order

Attend this highly timely panel, featuring top CISOs, coming just weeks after many new cybersecurity reporting requirements mandated by the White House Executive Order are due and weeks before the new 2018 fiscal government year begins. Fresh off these assessments and looking at the beginning of the government fiscal year, what are the top lessons CISOs have learned in 2017 and the top priorities for 2018? Benefits of attending this session include:

- Hear the upcoming priorities of top CISOs going into FY 2018
- Discover what solutions industry or government may need to craft to meet those priorities
- Find out how industry can provide products and solutions to best meet CISOs' priorities

Moderator:

- (b) (6) US CISO; President, Cyxtera Federal Group, Cyxtera Technologies

Speakers:

- (b) (6) for Cybersecurity, CIO, U.S. Department of Defense
- (b) (6) for Cyber Security and CISO, U.S. Department of the Treasury
- (b) (6) Information Security, U.S. Department of Health & Human Services
- (b) (6) Office of the CIO, U.S. Department of Homeland Security
- (b) (6) Northrop Grumman

9:30 – 10:00 am Break

10:00 – 10:20 am Keynote: A Look Inside Threats To Our Critical Infrastructures: Preparing For The Next Attack

Electricity, internet, gas, and water are of paramount importance in our everyday lives. Our dependence on these resources is particularly evident during even brief outages. To date, cyber attacks against critical infrastructures we've seen have been extremely sophisticated and unique to the nation-state actors often behind these incidents. In this presentation we will challenge this perception, showing that there is a common evolutionary path amongst the U.S., Russia, Iran, and North Korea that applies to any other nation-state targeting critical infrastructure. We will also examine the types of vulnerabilities and attacks used to target critical systems, the

complexities of securing these systems, and how organizations need to approach their security moving forward.

- (b) (6) FireEye's Mandiant Consulting

10:20 – 10:50 am Inside the Latest Emerging Cyber Threats—Tackling Spear Phishing, the Insider Threat, Ransomware, and IOT

Cybersecurity is evolving so rapidly that today's major cyber breach or attack quickly becomes yesterday's news. By September 13, the date of the conference, CISOs will undoubtedly be facing a new set of cybersecurity challenges. Hear this panel offer their insider perspectives on the cyber challenges and what looms on the horizon. With the explosion of IOT and mobile, the attack surface is growing; the attackers are growing in number and sophistication; and the threats are evolving. Hear leading experts in government and industry as they give you the most up-to-date information and analysis so you will come away better educated to respond.

- What threats are facing you in your organization on September 13?
- What are the evolving and emerging dangers?
- What prevention techniques are needed?

Moderator:

- (b) (6) Booz Allen Hamilton

Speakers:

- (b) (6) Cybersecurity Threat Operations Center, National Security Agency
- (b) (6) Cyber Threat Intelligence Integration Center, Office of the Director of National Intelligence
- (b) (6) Cybersecurity Strategy and Global Policy, Palo Alto Networks
- (b) (6) National Cybersecurity and Communications Integration Center, DHS

10:50-11:10 am Keynote – Understanding the cloud threat surface; Users are the new perimeter!

With government cloud adoption accelerating at an exponential pace, the traditional concept of a self-contained network with a defined perimeter is no longer valid. Users are now the perimeter, taking advantage of self-provisioning capabilities enabled by BYOx and cloud phenomena. This transformation is compounded by users augmenting core SaaS applications by self-selecting third-party apps, as well as the applications organizations build for themselves in the cloud. With

FOR OFFICIAL USE ONLY

the concept of a perimeter dissolving away, understanding what the cloud threat surface looks like and what it takes to detect a cloud breach is imperative.

- (b) (6) Head of Innovation, Cloud Security, Cisco

11:10 – 11:25 am Transition to Breakouts

11:25 am – 12:10 pm

Breakout 1: [CDM] CDM: How Government Can Leap Ahead and Industry Can Benefit in FY 2018 (Ballroom A, Level 3)

- A convergence will take place in 2017 & 2018 that has been long awaited:
 - US government funding and contract mechanisms will be available for Departments and Agencies to procure cybersecurity solutions under CDM,
 - Innovative private sector solutions could greatly increase the cybersecurity sophistication, while reducing the management complexity, of government systems.

CDM, now in its 4th year, is aimed at safeguarding cyberspace and protecting the cyber infrastructure of the civilian .gov network environment. The CDM Program moves away from historical compliance reporting toward combating threats on a real-time basis with state-of-the-art tools. This panel will examine the future of the CDM program and how industry can play a vital role.

Moderator:

- (b) (6) Cyber Solutions, Cyber and Intelligence Mission Solutions Division, Northrop Grumman Mission Systems

Speakers:

- (b) (6) Network Security Deployment, U.S. Department of Homeland Security
- (b) (6) FEDSIM, Dept. of Homeland Security
- (b) (6) Cyber Futures Group, Booz Allen Hamilton
- (b) (6) for the Public Sector, RSA
- (b) (6) Security Solutions, Adobe

Breakout 2: [NIST] Your Deep Dive in the NIST Framework: Best Practices and Lessons Learned (Room 143 A-C, Level 1)

As the government moves from a compliance to a risk management-based cybersecurity system, the NIST Framework is central. With the deadline for the agencies' reports for the NIST

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

Cybersecurity Framework due in August, September will be an important time to assess various agencies' progress as they look to FY 2018.

- What best practices and lessons learned will Federal and state government CISOs have to share in measurement and customizing the Framework for their organizations?
- What challenges lie ahead?

Moderator:

- (b) (6) of Strategy, Bay Dynamics

Speakers:

- (b) (6) U.S. Department of Agriculture
- (b) (6) California
Department of Technology
- (b) (6) Cybersecurity Framework, National Institute of
Standards & Technology
- (b) (6) Penn State Health &
College of Medicine
- (b) (6)
Bureau of Fiscal Services, U.S. Department of the Treasury

Breakout 3: [Threat Intel] Beyond Information Sharing to Shared Threat Intelligence: Best Practices and New Models from Government (Room 144 A-C, Level 1)

Cyber threat analysis is coming into increasing prominence as a recognized component of a comprehensive cybersecurity posture. However, 'cyber intelligence' continues to have multiple definitions and support multiple missions. This panel will present perspectives on this emerging field from government officials who support cyber threat analysis within the homeland security, law enforcement, military, and intelligence community mission areas. These thought leaders will talk about the supporting strategic and tactical requirements and their respective communities' relationship with the private sector on threat intelligence, providing actionable ideas for improvement.

Moderator:

- (b) (6) Booz Allen Hamilton

Speakers:

- (b) (6) Office of the Director of
National Intelligence

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

- (b) (6) Federal Bureau of Investigation
- (b) (6) Darktrace
- (b) (6) DoD Cyber Programs, Lockheed Martin

Breakout 4: [Endpoints] Endpoints Don't Have To Be The End Of Network Security (Room 140A, Level 1)

Endpoints are unquestionably the most vulnerable areas of most networks: A. because attackers now have a vast array to choose from and B. their security often relies on easily avoidable upgrades by an overwhelmed user. As such, endpoint security and threat detection are more critical than ever, as the perimeter becomes obsolete and 'all things connected' escalate attack vectors. How do you mitigate endpoint vulnerabilities that seem to grow like wildfire? Hear industry security experts share suggestions, successes and failures we can all learn from.

Questions to be addressed:

- How are industry leaders addressing the cybersecurity challenges posed by the Internet of Things?
- How best can the endpoints be secured as more is moved to the cloud and as mobile advances?
- What are the industry trends and the threat vectors across all segments?
- What recent endpoint attacks should you be aware of?

Moderator:

- (b) (6) Cyber adAPT

Speakers:

- (b) (6) Qadium, Inc.
- (b) (6) Exelon Corporation
- (b) (6) Fortinet
- (b) (6) Office of Cybersecurity, U.S. House of Representatives
- (b) (6) US Federal, Check Point Software Technologies

Breakout 5: [Crowdsourcing] Fireside Chat: Crowdsourcing Security Risk Assessment (Room 140B, Level 1)

Cybercriminals have never been so notorious. As technology innovation seems to outpace security defenses, organizations, including the U.S. Department of Defense, are turning to

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

ethical-hackers to assess risk and see where they are most vulnerable. Can these external hackers be trusted? Hear from leading experts about the misconceptions of working with hackers, what vulnerabilities are most common and how these programs can be used to manage and assess risk.

Questions to be answered:

- What do you need to know before inviting hackers?
- Can these external hackers be trusted?
- Can hackers help fill the cybersecurity skills gap?

Speakers:

- (b) (6) HackerOne
- (b) (6) Dept. of Defense
- (b) (6) Dept. of Defense

12:10 – 1:15 pm Lunch

1:15 – 1:45 pm Lunch Keynote: White House Cybersecurity Priorities

- (b) (5), (b) (7)(E), The White House

1:45 – 2:05 pm Keynote: The UK National Cyber Security Strategy and the National Cyber Security Centre: One Year On

- Conrad Prince, UK Cyber Security Ambassador

2:05 – 2:25 pm Keynote: Australian Cyber Affairs Priorities

- (b) (6) Australian Ambassador for Cyber Affairs

2:25 – 2:55 pm Emerging Technologies in Cybersecurity

What are the latest cutting edge technologies in cybersecurity and the greatest needs?

Moderator:

- (b) (6) Enterprise Security Solutions, Enterprise Services, U.S. Public Sector, DXC Technology

Speakers:

- (b) (6) Cyber Security Products, Cyber and Electronic Warfare Systems, General Dynamics Mission Systems
- (b) (6) of Technology, In-Q-Tel

FOR OFFICIAL USE ONLY

FOR OFFICIAL USE ONLY

- (b) (6) Adobe
- (b) (6) Bugcrowd

2:55 – 3:20 pm Dessert Break

3:20 – 3:40 pm Keynote

- Representative William Hurd, R-Texas

3:40 – 3:55 pm Keynote

- (b) (6) Office of Management and Budget (invited)

3:55 – 4:30 pm Top DOD Cyber Priorities for FY 2018 and Beyond

Hear some of the top military and civilian CIOs and their deputies who will be at the forefront as the government works to implement the requirements of the President’s Cybersecurity Executive Order. What are their chief priorities for FY 18 and beyond?

Moderator:

- Ra (b) (6) Tanium

Speakers:

- (b) (6), US Cyber Command
- (b) (6), US Air Force
- (b) (6), U.S. Army

4:30 – 5:00 pm Closing Keynote

- (b) (6), United States Central Command

5:00 – 5:05 pm Closing Remarks

- (b) (6)

FOR OFFICIAL USE ONLY

Critical Infrastructure Designation Tick Tock:

Thursday, January 5

- 2:45 pm: Call with National Association of Secretaries of State Working Group Members & EAC Commissioners
- 3:45: National Association of Counties & National Association of County Recorders, Election Officials & Clerks

Friday, January 6

- 9:15 am: Embargoed OLA notifications
- 9:30 am: Secretary Johnson issues statement
- 9:30 am: Stakeholder message

Press Release

October 7, 2016

JOINT STATEMENT FROM THE DEPARTMENT OF HOMELAND SECURITY AND OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE ON ELECTION SECURITY

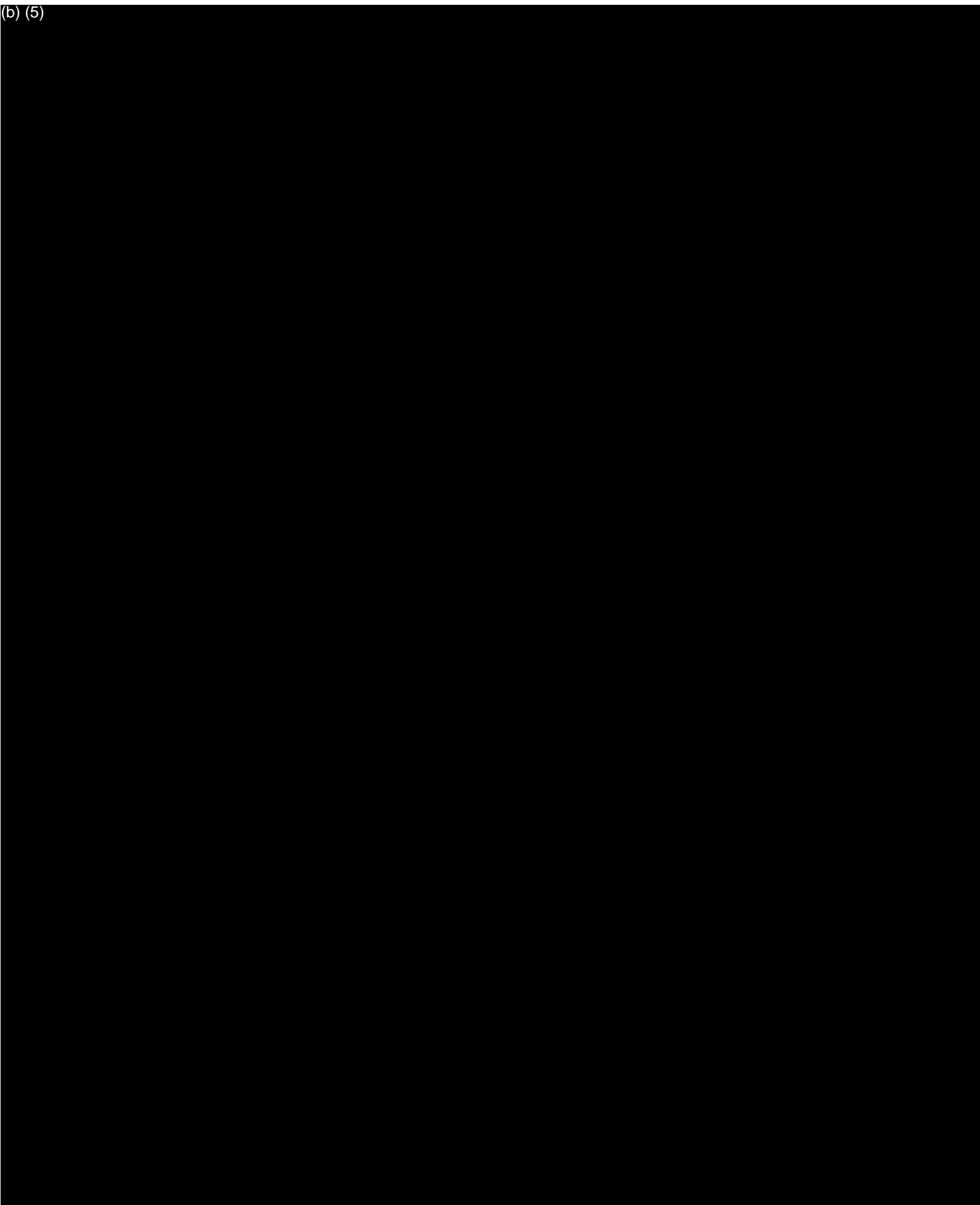
The U.S. Intelligence Community (USIC) is confident that the Russian Government directed the recent compromises of e-mails from US persons and institutions, including from US political organizations. The recent disclosures of alleged hacked e-mails on sites like DCLeaks.com and WikiLeaks and by the Guccifer 2.0 online persona are consistent with the methods and motivations of Russian-directed efforts. These thefts and disclosures are intended to interfere with the US election process. Such activity is not new to Moscow—the Russians have used similar tactics and techniques across Europe and Eurasia, for example, to influence public opinion there. We believe, based on the scope and sensitivity of these efforts, that only Russia's senior-most officials could have authorized these activities.

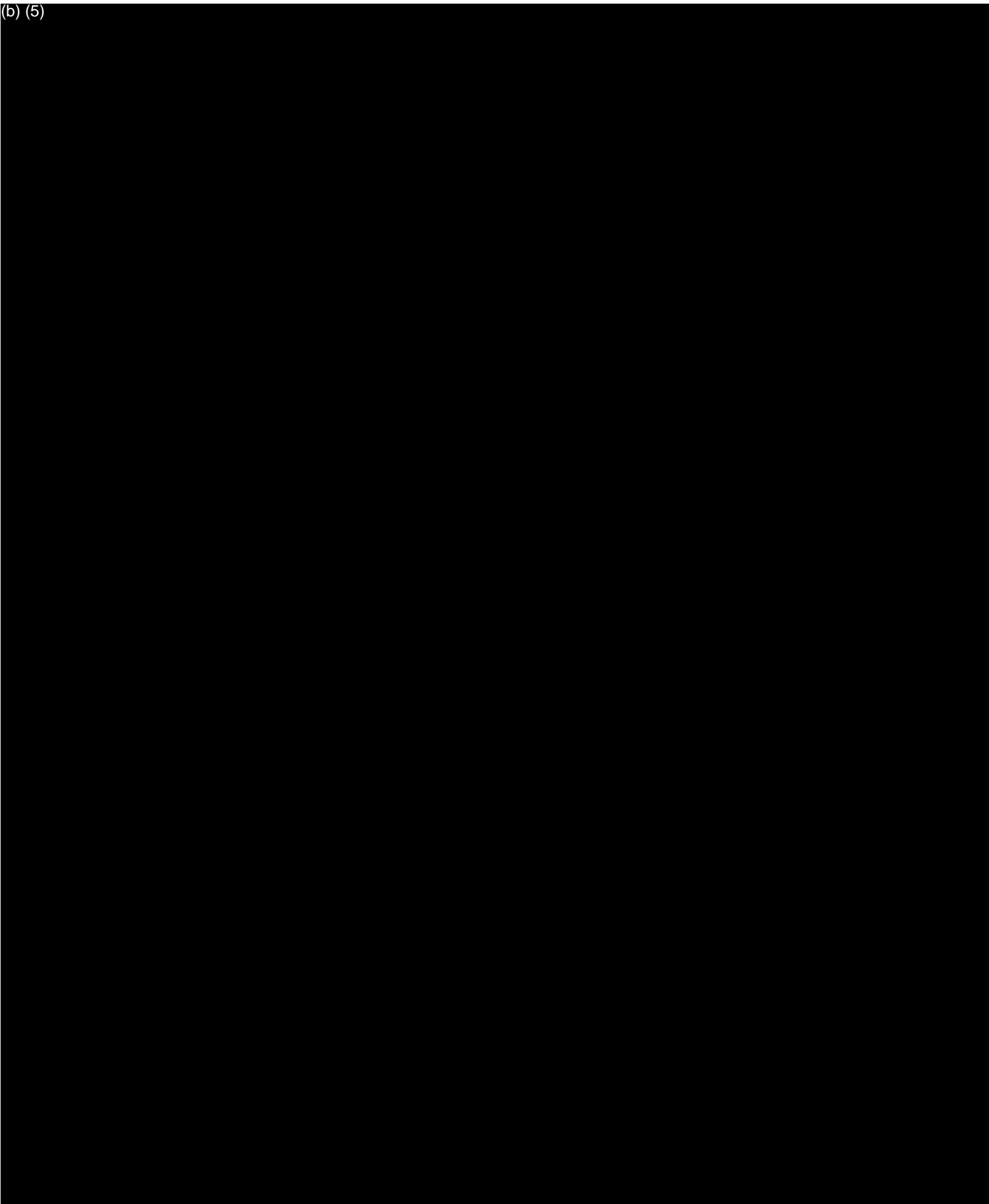
Some states have also recently seen scanning and probing of their election-related systems, which in most cases originated from servers operated by a Russian company. However, we are not now in a position to attribute this activity to the Russian Government. The USIC and the Department of Homeland Security (DHS) assess that it would be extremely difficult for someone, including a nation-state actor, to alter actual ballot counts or election results by cyber attack or intrusion. This assessment is based on the decentralized nature of our election system in this country and the number of protections state and local election officials have in place. States ensure that voting machines are not connected to the Internet, and there are numerous checks and balances as well as extensive oversight at multiple levels built into our election process.

Nevertheless, DHS continues to urge state and local election officials to be vigilant and seek cybersecurity assistance from DHS. A number of states have already done so. DHS is providing several services to state and local election officials to assist in their cybersecurity. These services include cyber “hygiene” scans of Internet-facing systems, risk and vulnerability assessments, information sharing about cyber incidents, and best practices for securing voter registration databases and

addressing potential cyber threats. DHS has convened an Election Infrastructure Cybersecurity Working Group with experts across all levels of government to raise awareness of cybersecurity risks potentially affecting election infrastructure and the elections process. Secretary Johnson and DHS officials are working directly with the National Association of Secretaries of State to offer assistance, share information, and provide additional resources to state and local officials.

(b) (5)





National Cyber Incident Response Plan

Final Release

December 2016



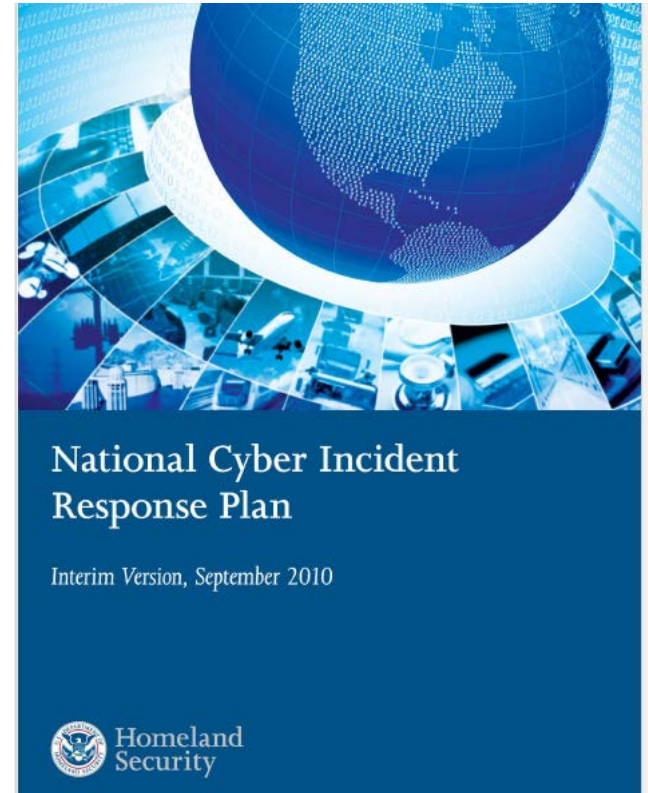
Homeland
Security

NCIRP Update Overview and Status

National Cyber Incident Response Plan (NCIRP) Document Overview

The NCIRP formalizes the structure and process for a whole community approach to mitigating, responding to and recovering from a significant cyber incident that impacts critical infrastructure.

- The NCIRP is ***not*** a tactical or operational plan for responding to cyber incidents.
- Instead, it serves as the primary strategic framework for stakeholders to use when developing ***their own*** agency, sector and organization-specific operational plans.



Roles and Responsibilities

- The NCIRP describes the whole community's roles and responsibilities during a cyber incident, including Federal, SLTT, private sector, and international stakeholders.
- NCIRP response activities are undertaken through four concurrent lines of effort:
 - Threat response (FBI lead);
 - Asset response (DHS lead);
 - Intelligence support and related activities (ODNI lead); and
 - Affected entity's response efforts
- International coordination plays a key role through all the lines of effort
- The Cyber Unified Coordination Group CONOPS details the process in how the incident response group will activate, coordinate, and stand down during a significant cyber incident.



Key Changes

The NCIRP:

- **Codifies** a national coordination process for cyber incident response
- **Reinforces** the need for strong connections and public-private partnerships
- **Improves** coordination, engagement, and working relationships
- **Aligns** more closely to the National Preparedness System
- **Fosters** stronger relationships between state fusion centers, risk managers, and chief information security officers



Status Updates

- To successfully draft and submit the NCIRP and Cyber UCG CONOP within that 180-day deadline, the National Protections and Plans Directorate (NPPD) through the Office of Cybersecurity and Communications (CS&C) dedicated a small group of staff and worked at an accelerated pace with a NCIRP Writing Group consisting of government and private sector partners.
- DHS held weekly writing sessions from June thru November to concurrently draft both documents and facilitated continued feedback throughout the development process. During the 30-day National Engagement Period this past October, CS&C received and adjudicated over 800 comments from the public and private sector.



Status Updates

- The National Cyber Incident Response Plan (NCIRP) and Cyber Unified Coordination Group (UCG) Concept of Operations (CONOP) were both approved by senior interagency leadership at the December 8th Cyber Response Group (CRG) and was sent to Department Deputies December 19th in a paper Deputies Committee package for awareness.
- The final Plan and CONOPS is being routed for transmission to the White House through Lisa Monaco and Shawn Donovan per the Presidential Policy Directive 41 (PPD-41) tasking. We anticipate full delivery by early January after final DHS approval which would be 3 weeks ahead of the 180-day deadline of January 22, 2017.
- Official announcement and awareness activities in early January pursuant to Department requirements.





SNAPSHOT OF OUR WORK

NPPD works with partners at all levels of government, and from the private and nonprofit sectors, to share information and build greater trust to make our cyber and physical infrastructure more secure and resilient.

On a typical day, NPPD employees:

- Issue more than 60 actionable cybersecurity alerts to the private sector and general public to help protect against threats.

- Work with State and local officials to plan security for large public gatherings, such as professional sporting events, July 4 celebrations, and marathons.

- Meet with dozens of owners and operators—from chemical plants and electric utilities to shopping malls—to help them assess and mitigate potential risks from terrorist attacks and natural disasters.

- Protect more than 9,000 Federal facilities and keep out more than 1,700 prohibited or illegal items.

- Process nearly 300,000 biometric identity transactions and verify approximately 7,000 derogatory matches in a timely and secure manner.

OVERVIEW

Established: 2007
Employees: 3,500
Field Offices: 230 cities
IP Regional Directors: 10
Protective Security Advisors: 102
Chem. Facility Inspectors: 147
Law Enforcement Officers: 900
Total Field Personnel: 1,500

Who We Are, What We Do

America has always been a nation of communities and neighborhoods, of relationships, values, and laws. Today, we're also a nation of networks and systems, ones we rely on for just about everything we do—from communicating and traveling to banking and shopping.

But the infrastructure that supports all of this—that enables our way of life—is vulnerable. It's vulnerable to an ever-evolving range of threats, from terrorist or cyberattacks to natural disasters, like hurricanes or floods.

That's where NPPD comes in. Why? Because reducing the risks from these threats and making our physical and digital infrastructure more resilient and secure is our abiding mission. Every day, the men and women of NPPD work across DHS and around the country to strengthen the very backbone of our national and economic security.

Often, NPPD is behind the scenes, making sure that the systems and networks Americans rely on are there when we need them.

In the homeland security world, as DHS Secretary Johnson has said, "No news is good news." For NPPD, no news is the result of hard work, vigilance, and dedication by people working to prevent bad things you never hear about, or help the public prepare itself and recover from the storm we cannot prevent.



DHS Secretary:
DHS Deputy Secretary (acting):
Under Secretary, NPPD:
Deputy Under Secretary, NPPD:
Deputy Under Secretary, Cybersecurity & Communications:
Chief of Staff, NPPD:
Assistant Secretary, Cybersecurity & Communications:
Assistant Secretary, Infrastructure Protection:
Director, Federal Protective Service:
Director, Office of Biometric Identity Management (acting):
Director, Office of Cyber and Infrastructure Analysis:

Jeh Johnson
Russ Deyo
Suzanne Spaulding
Dr. Ronald Clark
Dr. Phyllis Schneck
David Hess
Dr. Andy Ozment
Caitlin Durkovich
L. Eric Patterson
Shonnie Lyon
Brandon Wales



Key NPPD Offices

Federal Protective Service (FPS) is a Federal law enforcement agency that provides integrated security and law enforcement services to Federally owned and leased buildings and facilities.

Office of Biometric Identity Management (OBIM) is the DHS enterprise-wide provider of biometric identity services, providing accurate and timely biometric identity information while protecting the privacy and civil liberties of individuals.

Office of Cyber and Infrastructure Analysis (OCIA) provides integrated, all-hazards consequence analysis to illuminate the interdependence of our Nation's cyber and physical critical infrastructure.

Office of Cybersecurity and Communications (CS&C) has the mission of ensuring the security, resiliency, and reliability of the Nation's cyber and communications infrastructure.

Office of Infrastructure Protection (IP) leads the coordinated national effort to reduce risk to our critical infrastructure and help respond and quickly recover in case of terrorist attacks, natural disasters, or other emergencies.

Office of the Under Secretary (OUS) works with liaisons across NPPD and provides Directorate leadership, oversight, and support for our more than 3,000 employees nationwide.

Performance Highlights, FY 2016

- Conducted more than 200 classified and unclassified meetings with critical infrastructure partners to share actionable information and recommend preventative measures.
- Received approximately 56,000 cyber incident reports from Federal and critical infrastructure stakeholders. Conducted 17 on-site responses to cyber incidents and identified over 64,000 cybersecurity vulnerabilities through scans and vulnerability assessments.
- Deployed EINSTEIN 3 Accelerated (E3A) capabilities that have the capacity to protect 500,000 Federal users from malicious e-mail attacks (such as e-mail-initiated spear phishing campaigns) or malware installed on .gov networks.
- Conducted more than 1,700 Homeland Security initiative events since February.
- Conducted 28 in-person workshops in 24 states with 3,500 stakeholders. More than 120,000 stakeholders completed the online active shooter training.
- Under the Chemical Facility Anti-Terrorism Standards (CFATS) program, successfully approved more than 2,600 Site Security Plans or Alternative Security Programs for high-risk chemical facilities, and conducted more than 2,800 authorization and 1,100 compliance inspections to date.
- In response to a series of high profile attacks targeting government facilities and officials overseas, NPPD initiated surges of law enforcement and security experts at Federal government buildings in several cities. These operations enhanced the immediate security of 189 facilities and over 87,000 tenants.
- Processed over 88 million total transactions with more than 2.7 million watchlist identifications, including 350,754 Known Suspected Terrorist matches identified. Completed more than 4.4 million latent fingerprint comparisons and provided 2,318 identifications.
- Completed over 250 communications interoperability technical assistance engagements in 54 states and territories, including broadband consultation preparation and communications interoperability workshops. Supported states and territories in developing Interoperable Emergency Communications



LEARN MORE & PARTNER WITH US

See how your organization or business can work with NPPD:

dhs.gov/cyber

dhs.gov/critical-infrastructure

Summary
Hearing before the Senate Committee on Armed Services
“Foreign Cyber Threats to the United States”

On January 5th, 2017, the Senate Committee on Armed Services held a hearing to explore the various foreign cyber threats to the United States. Three witnesses participated in the hearing:

- James Clapper - Director of National Intelligence;
- Admiral Mike Rogers - Commander of the United States Cyber Command, Director of the National Security Agency, and Chief of the Central Security Services; and
- Marcel J. Lettre – Under Secretary of Defense for Intelligence.

It appears that most members of the Committee attended the hearing. However, due to time restraints, some of the more junior Committee members were not able to question the witnesses. Most inquiries were directed at Director Clapper and Admiral Rogers. While some Senators used their time to discuss general foreign cyber threats, most focused on Russia’s interference in the 2016 US presidential election.

Chairman John McCain (R-AZ), Ranking Member Jack Reed (D-RI), and Senator Tim Kaine (D-VA) asked questions to confirm previously-released information related to the 2016 election. The Intelligence Community (IC) still believes that the Russian government authorized and led the efforts. This involved cyber attacks on systems used by players in the election, as well as the spread of propaganda. However, there is no evidence that any votes were changed by the hackers. (As Senator Martin Heinrich [D-NM] stated during his allotted time, interference does not always equal stuffing ballot boxes). The IC is developing a classified report on their findings as they related to both the cyber and propaganda aspects of the Russian’s actions, which will be briefed to Members of Congress, the President, and the President-Elect. An unclassified version will be made available to the public. The report will cover the full range of methods used by the Russians in their efforts. Director Clapper, in responding to questions from Senators McCain and Joe Donnelly (D-IN), stated that confidence is “very high” within the IC that the actions have been correctly attributed to the Russians.

The largest focus of many questions was how best to respond to a cyber attack like the Russian’s intrusions last year. Senator McCain, also a member of the Senate Committee on Homeland Security and Governmental Affairs (HSGAC), asked if there was a policy in place to respond to a cyber attack. Under Secretary Lettre stated that the right levels of deterrence and response need to be determined before that policy could be developed. Senator Bill Nelson (D-FL) asked, if a recently reported incident related to a utility’s network in Vermont had actually been a cyber attack, how would the U.S. respond? Director Clapper said that responses could include sanctions or retaliatory cyber attacks, but that it would be “situationally dependent.” However, the U.S. government has to be careful to not spark a counter-retaliation. Senator Roger Wicker (R-MS) noted that there seems to be no real discussion of using retaliation as an appropriate deterrence for others when considering whether to launch a cyber attack against the United States. Director Clapper said that such discussions are happening at the highest level of the Federal Government, but that many legal issues have to be taken into account when considering any retaliatory actions. Senator Dan Sullivan (R-AK) asked if collapsing a country’s financial market would send the right message to an adversary that had launched a cyber attack. Under Secretary Lettre said that, again, the right level of retaliation must be considered for the scenario. Senator Lindsay Graham (R-SC) stated that he believed that the sanctions imposed on Russia by

Hirono, that a greater flexibility in compensation might help stem the flow of staff to the private sector. Senator Tillis also noted an interest in working with Admiral Rogers on recruiting and retaining members of the cyber workforce.

Shortly before the election, some in Congress asked if the Nation's election infrastructure should be designated as critical infrastructure. Senator Gillibrand brought this topic up in her questioning of Director Clapper, asking for his thoughts on the designation. He said that such a designating has been greatly discussed within the Administration, but that there had been "some pushback." He was not clear on where the pushback was coming from. Director Clapper said that it was not for the Intelligence Community to make the determination. Senator Gillibrand seemed open to such a designation.

Spreading information was noted as a major issue in cybersecurity during the hearing, both in terms of information sharing with partners and in Russia's propaganda program. Senator Fischer was the only Senator to ask about the *Cybersecurity Information Sharing Act of 2015* (DHS engaged heavily with Congress during the drafting of this bill). She asked how the law was being implemented, especially in relation to public-private information sharing. Director Clapper noted that the Federal Government was working on this issue before the law was signed, working with fusion centers to get information to the state and local agencies. Admiral Rogers stated that information may flow better to some sectors than others and that the products delivered by the IC may not be best optimized for sharing actionable information with the private sector. In response to a previous question from Senator Inhofe, Director Clapper stated that the Intelligence Community engages with all critical infrastructure groups to better secure their networks and systems. Senator Jeanne Shaheen (D-NH) asked if the Intelligence Community had a strategy to respond to Russia's propaganda spreading activities. Director Clapper, as he had previously said in responding to a comment from Senator McCain, discussed the need for a United States Information Agency "on steroids" to fight the information being spread. When asked by Senator Shaheen why this strategy had not been developed yet, Admiral Rogers said that the government may not have come to a full recognition that things needed to be done differently.

Senators Claire McCaskill (D-MO) and Richard Blumenthal (D-CT) used their time to discuss recent comments on the Intelligence Community's ability to attribute these attacks to the Russian government. In her line of questioning, Senator McCaskill, who is the HSGAC Ranking Member, pointed to the apolitical nature of the work that the IC does. Director Clapper agreed that the community is, and should remain, completely apolitical. Senator Blumenthal's questioning led Director Clapper to state that public trust and confidence in the Nation's intelligence agencies is crucial – not just here, but abroad. Senator Heinrich asked about the effect of these comments on Intelligence Community staff. Admiral Rogers stated that he was concerned about losing people because they feel like their professional value is being questioned.

Senators McCain, Fischer, and Shaheen discussed the legislative aspects of U.S. cybersecurity efforts. Senator McCain asked about the effect of the overlapping Congressional committee jurisdiction that the IC has to engage with. Director Clapper would not provide a direct opinion; however, Admiral Rogers noted that an integrated approach to providing oversight would be helpful. Senator Fischer asked Admiral Rogers if he needed any new statutes to be able to improve the NSA and Cyber Command's capabilities or if the organizations needed to just improve their abilities. He responded that both are necessary. Senator Shaheen asked if there is a need to reform the Office of the Director of National Intelligence. While Director Clapper said

President Obama were like “pebbles” and that he preferred to throw a “stone.” Senator Heinrich stated his concern that attacks like this would happen again if a high cost was imposed. He asked Under Secretary Lettre about the importance of tools like sanctions when responding to an attack. While noting the importance of sanctions, the Under Secretary said that it was important to consider all tools for imposing costs.

Using a previous cyber incident in his line of questioning, Senator James Inhofe (R-OK) asked if any actions were taken after the Office of Personnel Management (OPM) breach last year. Director Clapper said that the Intelligence Community had worked with OPM to enhance its cyber posture. However, he noted that the OPM hack was more espionage than an attack. In a previous question from Senator McCain, Director Clapper said that the Russian’s cyber attack had “great gravity,” but could not say if it was actually an act of war. Admiral Rogers stated that massive collections of data have a higher target value in an act of espionage. Later in the hearing, however, in responding to Senator Ted Cruz’s (R-TX) questioning on the greatest cyber threats, Admiral Rogers said that he worried about hackers extracting data from these huge collections for commercial benefit or operational degradation, as well as manipulating data to cause incorrect analysis.

While many Senators focused on how best to retaliate against these and similar attacks, there were some questions on how best to deter and mitigate the effects of a cyber attack launched from a foreign nation. Senator Wicker asked if the government has any way to effectively deter someone from launching a cyber attack against the United States. Director Clapper said that, right now, he does not believe that there is one truly effective way. In responding to a question from Senator Sullivan, Director Clapper said that many nations do not see the costs of cyber intrusions to be high enough to deter their efforts. Therefore, they continue to push the boundaries of their abilities. Senator Thom Tillis (R-NC) asked if occasionally exposing our presence in various foreign networks might serve as a deterrent, similar to placing physical military equipment when adversaries can see them. Director Clapper said that that could, in fact, act as a deterrent.

Some questions and responses focused on coordinating with other countries in dealing with cyber attacks. Director Clapper responded in the affirmative when asked by Senator Reed if Russia is engaging in similar electoral intrusions in Europe. Later, in responding to a question from Senator Cruz, Director Clapper said that Russia is looking to increase engagement in the Western hemisphere through intelligence and military coordination with countries such as Cuba and Venezuela. Senator Deb Fischer (R-NE) asked if, when determining “cyber norms,” should the U.S. attempt to build consensus internationally or focus domestically. Admiral Rogers noted that cyber does not recognize geographic boundaries and that the country must do both. Senator Mazie Hirono (D-HI) asked if countries like Russia and China would be key players in developing international cyber norms. Director Clapper noted this as part of the challenge in this effort, but noted that there is work being done at the United Nations to determine these norms.

Congress has shown much interest in the Federal Government’s ability to recruit and retain cyber professionals. This issue came up during multiple lines of questioning, along with the morale of these staff members. Senator Kirsten Gillibrand (D-NY) asked Admiral Rogers about the current state of recruiting cyber staff. He responded that, while recruitment and retention efforts in the military staff are exceeding goals, there have been issues in retaining staff on the civilian side. Both Admiral Rogers and Director Clapper said, in a response to a later question from Senator

that there is always room for improvements, the Office's statutory mandates much be considered and Congress consulted before any changes are made. At the end of the hearing, Senator McCain asked Director Clapper if he had any reflections on his time as Director of National Intelligence on the role of Congress in the Intelligence Community. He responded that, while Congress has an important role in overseeing intelligence agencies, there is a difference between oversight and micromanagement.