Elections Security Panel

MACO ANNUAL CONFERENCE – FEBRUARY 13, 2018

Agenda

- Panel Presentations
  - Secretary of State
  - Equipment Vendors
  - Department of Homeland Security
- Audience Q&A

Panel Members

- Gary Poser, Director of Elections, Minnesota Office of the Secretary of State
- Jessica Bowers, Manager, Certification Compliance, Dominion Voting Systems
- Adam Carbullido, Sr. VP, Product Development, Election Systems & Software
- Eddie Perez, Director of Product Management, Hart InterCivic
- Ken Terry, Project Manager, KNOWiNK
- Alex Joves, Regional Director, Office of Infrastructure Protection, Department of Homeland Security

Voter Registration Security

OFFICE OF MINNESOTA SECRETARY OF STATE

FEBRUARY, 2018

Online Security Assessments

- Yearly report to Legislature
- Use 3rd Party web application security firm
  - Seek score of 90 or higher (highest level)
- DHS scan/penetration testing

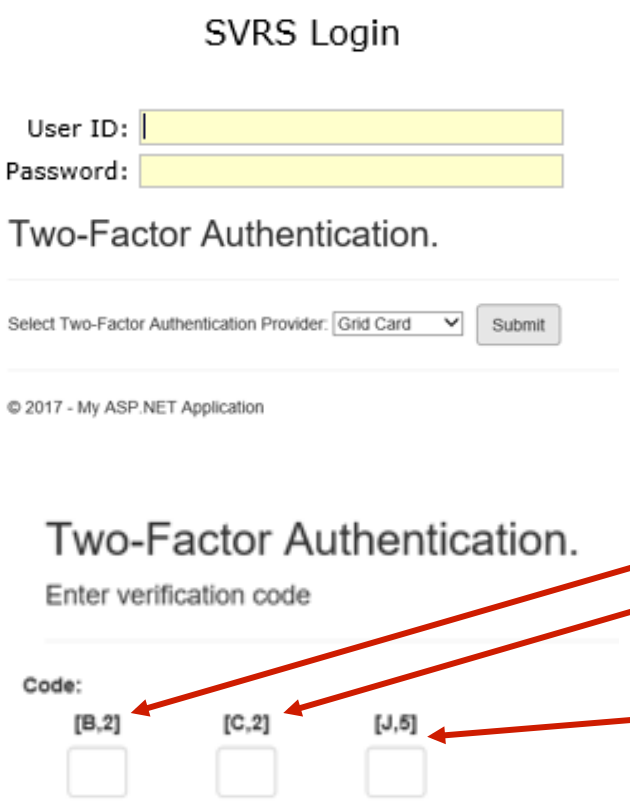
Security Info

- Data declared as Security Info are not public
  - Database design
  - Coding
  - Test scripts
  - Security and development methodology
- Firewalls and intrusion detection/prevention appliances

Multi-Factor Authentication

- SVRS will require 2nd Factor Authentication in Spring, 2018
- Many of your bank accounts may require something similar
- In addition to UserID and Password, a requested code must be input to fully log in
- All users will be issued a grid card similar to Bingo Card
  - (May opt to use smartphone app)
- During login, user will be asked to input number/letter corresponding to grid location

Multi-Factor Authentication



- During login, user is asked to input code from grid from coordinates:
- B-2
- C-2
- J-5

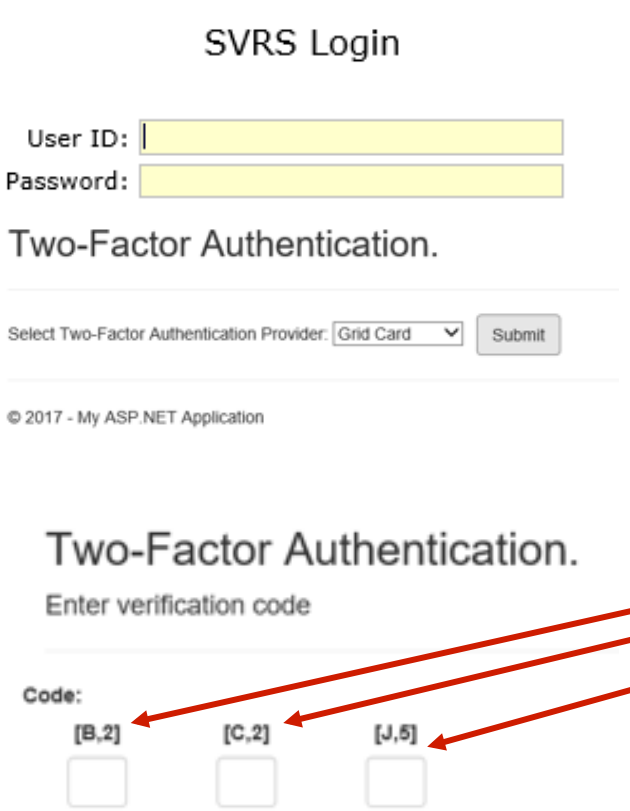
Card Grid

	A	B	C	D	E	F	G	H	I	J
1	5	1	3	C	E	T	1	0	J	Y
2	Q	E	P	C	K	C	D	V	M	4
3	Y	4	N	5	7	C	V	J	0	P
4	R	K	C	Q	7	T	M	H	H	C
5	1	9	K	T	J	5	T	3	V	V

Multi-Factor Authentication

- OSS assign current users a grid card; provide printed cards during deployment
- When creating new user in SVRS, create a user in Multi-Factor app with the same user name from SVRS
- Assign an unused grid card to the user
  - County will be provided extra grid cards
  - Can also generate/print new grid cards if needed
- Activate the grid card
- New user can log in to SVRS

Multi-Factor Authentication



- Optional app on users phone
- During login, select phone instead of grid card
- Access phone app to get code
- Input code into SVRS MFA fields

County Security Practices

- Secure access to SVRS through static IP address, not public wifi
- Separate Static IP address for elections vs other county depts
- Monitor not visible from counter
- Individual UserIDs, no shared UserIDs/passwords
- UserID, password not on post-it notes next to monitor
- Users assigned to appropriate SVRS-role (Auditor, Election Admin, Clerk, etc.)
- Disable inactive users

County Security Practices

- Beware of phishing/email scams
- Vote accumulation separate from internet-connected PC
- USB drives
- Printing lists with private data, destruction, email attachments

Dominion Voting Systems

JESSICA BOWERS

Election Systems & Software

ADAM CARBULLIDO

Hart InterCivic

EDWARD PEREZ

Securing Elections, Defense-In-Depth

Edward Perez
Director of Product Management
Hart InterCivic, Austin, Texas

Hart InterCivic

Austin, Texas
Since 1912
Voting technology in 18 states

Hart Voting System (first generation)
Verity (all-new, second generation, 2015)

Traditional paper ballots
By-Mail/high-speed scanning
Electronic and paper solutions

Newest system: Multiple EAC certifications, certified in 12 states

HART intercivic™

Security

Multi-layered approach
What are you trying to secure?
The “walled garden” & air gaps
Modern best practices
Holistic approach, “defense-in-depth”
- Data
- Access to data
- Presentation layer
- Workstations and devices

Auditability

Is the voting system working correctly, and how do I know?
Robust logging, plain language approach
Trace human-readable CVRs to individual paper records or images
Human-centered design
Transparency for stakeholders

HART intercivic™

KNOWiNK

KEN TERRY

Election Infrastructure Security

ALEX JOVES

Election Infrastructure Security Initiative

February 13, 2018

Elections: Critical to American Democracy

"Given the vital role elections play in this country, it is clear that certain systems and assets of election infrastructure meet the definition of critical infrastructure, in fact and in law."

– DHS Election Infrastructure Designation Statement, Jan. 6, 2017

- Critical infrastructure is defined as:

  "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."

What Is Critical Infrastructure?

- There are 16 critical infrastructure sectors:

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

DHS's Role In Critical Infrastructure

- The Homeland Security Act of 2002 created DHS and gave it responsibility for coordinating national critical infrastructure protection, including:
  - Work with state, local, tribal, and territorial governments, the private sector, and international partners;
  - Conduct risk assessments and identify priorities for protective measures;
  - Develop and maintain the National Infrastructure Protection Plan (NIPP).

National Infrastructure Protection Plan

- The National Infrastructure Protection Plan (NIPP) 2013 established a framework for national, coordinated efforts to protect critical infrastructure by managing risk in each of 16 sectors.
- NIPP's voluntary partnership model is the ***primary*** means of coordinating public and private sector infrastructure protection efforts through collaboration:

Sector-Specific Agency (SSA)	Coordinates security and resilience efforts in each sector.
Government Coordinating Council (GCC)	Forum for stakeholders from different levels of government.
Sector Coordinating Council (SCC)	Forum for private sector entities to work jointly among themselves and with the GCC and SSA.

Critical Infrastructure Designation Benefits

- Enables DHS to **prioritize assistance** to and resources for State and local government ***when*** and ***only if*** the officials request such assistance. (DHS only provides assistance if it is requested.)
- Enables secret level clearances to be given to state and local stakeholders.
- Allows frank discussions between DHS and stakeholders on vulnerabilities.
- Signals to domestic and international adversaries U.S. election infrastructure receives all the protections and benefits of critical infrastructure.
- Provides protection to specific information given to DHS under the Protected Critical Infrastructure Information Program from public and other disclosure.
- Establishes an Information Sharing Analysis Center (ISAC) to provide tailored cybersecurity analysis to officials.

What The Designation Does Not Do

- **Does not impose** any federal regulation or requirement on state and local operation or management of election infrastructure.
- **Does not give** DHS or any federal agency authority over state and local election infrastructure.
- **Does not require** state and local election officials to use DHS programs and services.

Election Infrastructure

Election infrastructure refers to assets, systems, and networks most critical to the security and resilience of the election process, such as:

- Storage facilities

- Polling places

- Voter registration databases, and the information technology infrastructure and systems used to maintain such databases.

- Information technology infrastructure and systems used to count, audit, and display election results.

DHS's Critical Infrastructure Partner Role

- DHS is the sector-specific agency (SSA) responsible to and for the Election Infrastructure Subsector (EIS).
- As its SSA, DHS remains a partner to, not an overseer of, state and local election officials, and supports the work of state and local election officials.
- DHS funds the Multi-State Information Sharing and Analysis Center to provide information services to state and local election officials.
- To further develop and support the state and local partnership, DHS created the Election Task Force (ETF) as part of a **whole-of-nation** approach to unify federal efforts to ensure security and resilience of election infrastructure.

DHS Employs A "Whole of Nation" Approach

- Securing election infrastructure is a national priority and no one entity can be successful working alone - it takes a "whole of nation" approach.
- Just as most critical infrastructure is not federally owned or managed, election infrastructure is outside federal control.
- DHS values and builds partnerships based on a foundation of trust, information sharing.

DHS Works With A Variety Of State and Local Partners

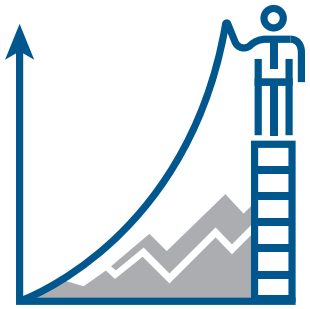
DHS works with partners in all levels of government:

ETF: Federal Support for Election Infrastructure

Formed in October 2017, the Election Task Force coordinates and synchronizes all federal activity on behalf of election infrastructure.

ETF's work is guided by three primary goals:

- **Understand threat and characterize risk** to election infrastructure to inform planning, resourcing, and prioritization of EI efforts.
- **Provide services** to EI stakeholders to help reduce both cyber and physical risk to state infrastructures, ensure access to actionable threat information, and maintain situational awareness of trends across the sector.
- **Mature** the organization of the EI Subsector to ensure a representative and effective security-informed partnership.



Election Task Force Members

EIS Government Coordinating Council

- Formed in October 2017, the EIS Government Coordinating Council (GCC) is a 27-member body of 24 state and local government representatives and 3 federal government representatives
- The EIS GCC:
  - Provides a forum for government to work jointly on an array of efforts to support election infrastructure through collective and individual expertise and resources.
  - Will receive classified threat information as well as threat and vulnerability information.
  - Will also help determine who else in the election community should receive that information so they are both recipients and involved in the sharing of information.

EIS Sector Coordinating Council

- Formation of the EIS Sector Coordinating Council (SCC) is underway.
- The EIS SCC will be a self-governing group, enabling private-sector critical infrastructure owners and operators and industry representatives to work jointly on sector-specific strategies, policies, and activities.
- The EIS SCC will coordinate and collaborate with the EIS GCC and DHS as its SSA to address critical infrastructure security and resilience policies and efforts for election infrastructure.

DHS Election Infrastructure Services

- DHS offers a broad range of services and programs to help secure election infrastructure.
- Services and programs are free, and all are voluntary and provided upon request.
- Contact Cybersecurity Advisors (CSA) or Protective Security Advisors (PSA) to discuss how to select, prioritize, and sequence available services and educational programs based on specific needs.

Cybersecurity Service Centers

Homeland Security

MS-ISAC
Multi-State Information Sharing & Analysis Center

24/7 cybersecurity operations centers that maintain close coordination among the private sector, government officials, the intelligence community, and law enforcement to provide situational awareness and incident response, as appropriate.

Contact Information

For more information on DHS cyber programs, visit www.dhs.gov/cyber

For access to the full range of DHS cyber resources, email SLTTCyber@hq.dhs.gov

To become an MS-ISAC member, visit www.cisecurity.org/ms-isac/

Summary of DHS Services:

Cybersecurity Assessments

Needs	DHS Services	Summary
Identify and Limit Vulnerabilities	Cyber Hygiene Scanning	Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis. As potential issues are identified DHS works with impacted stakeholders to mitigate threats and risks to their systems prior to their exploitation.
	Risk and Vulnerability Assessment (RVA)	• Penetration testing • Social engineering • Wireless access discovery • Database scanning • Operating system scanning
	Phishing Campaign Assessment	• Measures susceptibility to email attack • Delivers simulated phishing emails • Quantifies click-rate metrics over a 10-week period

Summary of DHS Services:
Cybersecurity Assessments, Cont'd

Needs	DHS Services	Summary
Cyber Risk and IT Security Program Assessment	Cyber Resilience Review (CRR)	One-day, onsite engagement conducted on an enterprise-wide basis to give insight on areas of strength and weakness, guidance on increasing organizational cybersecurity posture, preparedness, and ongoing investment strategies.
	External Dependencies Management Assessment	To access the activities and practices used by an organization to manage risk arising from external dependencies that constitute the information and communication technology service supply chain.
	Cyber Infrastructure Survey (CIS)	Assesses an organization's implementation and compliance with more than 80 cybersecurity controls.

Summary of DHS Services:

Physical Assessments

Needs	DHS Services	Summary
Identify and Limit Vulnerabilities	Assist Visit (AV)	On-site engagement to inform and educate owners and operators on threats from terrorism, the criticality of their facilities, and available Office of Infrastructure Protection (IP) and Department of Homeland Security (DHS) resources.
	Infrastructure Survey Tool (IST)	Facilitated survey to Identify and document critical infrastructure overall security and resilience, and provide information for protective measures planning and resource allocation.
	Hometown Security	A source for providing tools and resources to protect public gathering venues.

To learn more about our products and services, please visit https://www.dhs.gov/ecip and https://www.dhs.gov/hometown-security.

Summary of DHS Services:
Detect and Prevent

Needs	DHS Services	Summary
Detect Network Threats	Cyber Threat Hunting	Utilizes advanced hunting capabilities to identify adversary presence in a network that evades traditional security controls. For more information, call (888) 282-0870
Enhance Network Protection	Enhanced Cyber Services (ECS)	Intrusion prevention service to augment, not replace, existing cybersecurity capabilities. Leverages sensitive and classified cyber threat indicators to block malicious traffic from entering customer networks. Service offerings, available through accredited commercial service providers, include: • Domain Name Service (DNS) Sinkholing • Email (SMTP) Filtering • Netflow Analysis For more information, visit www.dhs.gov/enhanced-cybersecurity-services

Summary of DHS Services:

Information Sharing & Awareness

Needs	DHS Services	Summary
Cyber Alerts and Advisories	National Cyber Awareness System (NCAS)	Timely information about security topics and threats via subscription to a mailing list. NCCIC provides current activity, alerts, bulletins, and security tips to stakeholders. For more information, visit www.us-cert/gov/ncas
Collaboration	Homeland Security Information Network (HSIN)	The NCCIC portal provides stakeholders a platform to securely collaborate and share cybersecurity information, threat analysis and products within trusted communities of interest. For more information, contact HSIN.Outreach@hq.dhs.gov Connect to HSIN at https://auth.dhs.gov/oam/hsinlogin/HSINLogin

Summary of DHS Services:

Information Sharing & Awareness, Cont'd

Needs	DHS Services	Summary
Exchange of Cyber Threat Indicators	Automated Indicator Sharing (AIS)	Enables real-time bidirectional exchange of cyber threat indicators at machine speed, with the goal of reducing the number of cyber attacks. For more information, visit www.us-cert.gov/ais Share Indicators at www.us-cert.gov/forms/share-indicators
Applying Security Expertise and Best Practices	Cybersecurity Advisors (CSAs) & Protective Security Advisors (PSAs)	Regionally located personnel who engage state and local governments, election crime coordinators, and vendors to offer immediate and sustained assistance, coordination, and outreach to prepare and protect from cyber and physical threats. For more information, visit www.dhs.gov/protective-security-advisors

Summary of DHS Services:

Training & Education

Needs	DHS Services	Summary
Educational Material	Stop.Think Connect. Toolkit	Resources and materials to help promote cybersecurity awareness. Provides a better understanding of cyber threats and empowers people to be safer and more secure online. For more information, visit www.dhs.gov/stopthinkconnect
Career Development	Federal Virtual Training Environment (FedVTE)	Online and on-demand cybersecurity training system for Federal/ SLTT government personnel and veterans. Courses range from beginner to advanced levels. Training is accessible from any Internet enabled computer. For more information, visit https://fedvte.usalearning.gov
	National Initiative for Cybersecurity Careers and Studies Catalog (NICCS)	Catalog of more than 3,000 cybersecurity-related courses both online and in-person from more than 125 different providers across the nation. Courses are aligned to the specialty areas of the National Cybersecurity Workforce Framework. For more information, visit www.niccs.us-cert.gov/training

Summary of DHS Services:

Training & Education, Cont'd

Needs	DHS Services	Summary
Exercises & Planning	National Cyber Exercises and Planning Program (NCEPP)	Provide cyber exercise planning workshops and seminars, and conduct tabletop, full-scale and functional exercises for organizations to rehearse their response to staged incidents, allowing organizations to develop "muscle memory" and identify areas that may need to be improved in order to prepare for a real-world situation. For more information, contact CEP@hq.dhs.gov
	IP Stakeholder Readiness & Exercise Program	Conduct discussion- and operation-based exercises focused on enhancing critical infrastructure security and resilience. Provide resources for the critical infrastructure community to conduct independent tabletop exercises through the Sector-Specific Tabletop Exercise Program (SSTEP). For more information, contact SOPD.Exercise@hq.dhs.gov

Summary of DHS Services:

Physical Security Initiatives

Needs	DHS Services	Summary
Physical Security	IP Active Shooter Preparedness Program	Provide a comprehensive set of resources to position public and private sector organizations to reduce the impacts of an active shooter event. Includes in-person training, online training, and educational resources. For more information, contact ASWorkshop@hq.dhs.gov or visit www.dhs.gov/active-shooter-preparedness
	IP Unmanned Aircraft System (UAS) Initiative	Address threats posed to critical infrastructures from emergent adversary use of UAS. Offers policies and risk mitigation solutions for safe, secure, and beneficial use of UAS, associated countermeasures, and cyber/physical emerging technology analysis. For more information, contact IP-UAS@hq.dhs.gov

Summary of DHS Services:

Physical Security Initiatives, Cont'd

Needs	DHS Services	Summary
Physical Security	IP Soft Target Security Initiative	Provides national leadership on technology, standards, and best practices to demonstrably reduce the risk of successful attacks on soft targets. Serves as a center of gravity for DHS-wide resources available to support the critical infrastructure community in securing soft targets. For more information, contact IP-SoftTargetSecurity@hq.dhs.gov

Summary of DHS Services:

Incident Response

Needs	DHS Services	Summary
Analysis of Malicious Code	Advanced Malware Analysis Center	Provides 24/7 dynamic analyses of malicious code. Stakeholders submit samples via an online website and receive a technical document outlining the results of the analysis. Experts will detail recommendations for malware removal and recovery activities. This service can be performed in concert with Incident Response services, should the incident warrant the need. To submit malware for analysis, visit www.malware.us-cert.gov
Mitigation and Recovery	Incident Response	Provides 24/7 intrusion analysis in response to a cyber incident. Dispatches skilled personnel when a cyber incident occurs to assist in identifying malicious actors, technical analysis, containment, mitigation guidance, and post-incident recovery. Report an incident, at www.us-cert.gov/forms/report For more information, visit www.us-cert.gov

MS-ISAC
Multi-State Information Sharing & Analysis Center

- Provides cybersecurity support to SLTT governments.
- Furthers DHS efforts to secure cyberspace by distributing early warnings of cyber threats to SLTT governments.
- Shares security incident information and analysis.
- Runs a 24/7 watch and warning security operations center.
- Funded by DHS.

For more information, see https://www.cisecurity.org/ms-isac.

For more information:

- Glenn Sanders – DHS Protective Security Advisor (PSA) Minnesota
  - Glenn.Sanders@hq.dhs.gov
- Mike Christianson – DHS Protective Security Advisor (PSA) Minnesota
  - Michael.Christianson@hq.dhs.gov
- Tony Enriquez – DHS Cybersecurity Advisor (CSA) – Region 5
  - Antonio.Enriquez@hq.dhs.gov
- Alex Joves – DHS Infrastructure Protection Regional Director – Region 5
  - Alexander.Joves@hq.dhs.gov

Questions?