Homeland Security

Elections Systems: A Designated Critical Infrastructure

Unique designation that provides for a basis for the Department of Homeland Security and other federal agencies to:

- Recognize the importance of these systems,
- Prioritize services and support to enhancing security for such infrastructure,
- Afford the elections community an opportunity to work with each other and with the Federal Government, through government and private sector coordinating councils, and
- Communicate to the global community our intention to hold those responsible who attack these systems as violating international norms.

Election Infrastructure Subsector GCC

Federal, state, and local government partners formed the Election Infrastructure Subsector GCC (EI-GCC) and met for the first time in Atlanta, October 2017.

- Formation was a milestone in multi-level government cooperation and bolstered election infrastructure security and resiliency.

EIS GCC:

- Enables partners to leverage information sharing; physical/cyber products, resources, and capabilities; and collective expertise.
- Is a 27-member group, 24 of which are state and local election officials.
- Is led by a five-member Executive Committee (Chair: DHS/NPPD; EAC; a Secretary of State; a state election director; and a local election director) which meets bi-weekly.
- Sector specific plan adopted in 2018, sector priorities for 2019-2020 approved on February 1, 2019.

Election Infrastructure Subsector CC

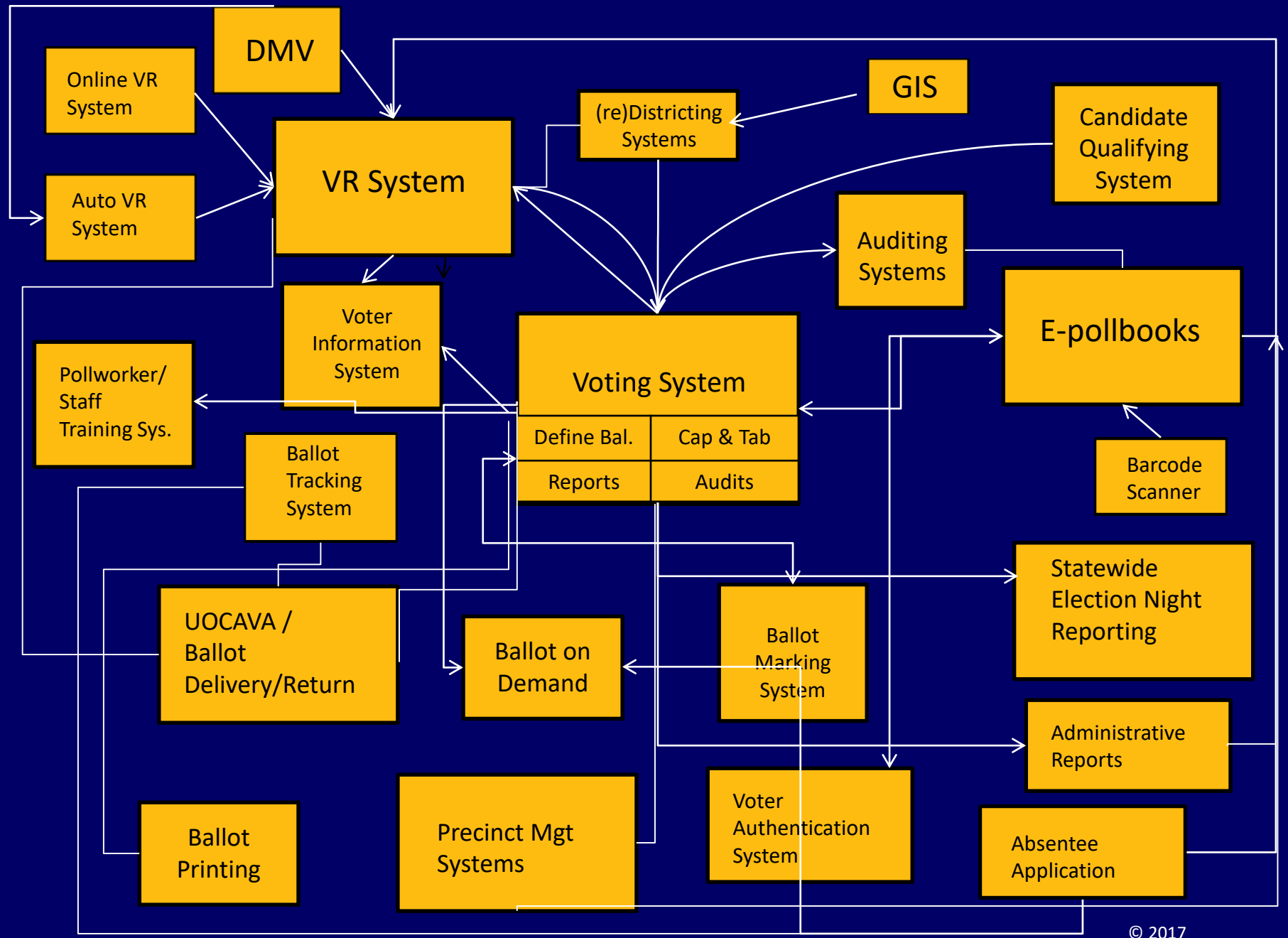
Private sector stakeholders formed the Election Infrastructure Subsector Coordinating Council (EISCC) and held first meeting February 2018.

- Led by a five-member Executive Committee.

EISCC responsibilities include:

- Serve as the primary liaison between the private sector and government on election infrastructure security.
- Facilitate information and intelligence sharing.
- Coordinate with DHS and the EI-GCC to develop, recommend and review sector-wide plans, procedures.
- Established action plan with goals and priorities in February, 2019.

Interaction of Voting and Election Systems



This slide is from the Belfer Center's State and Local Election Cybersecurity Playbook: https://www.belfercenter.org/publication/state-and-local-election-cybersecurity-playbook

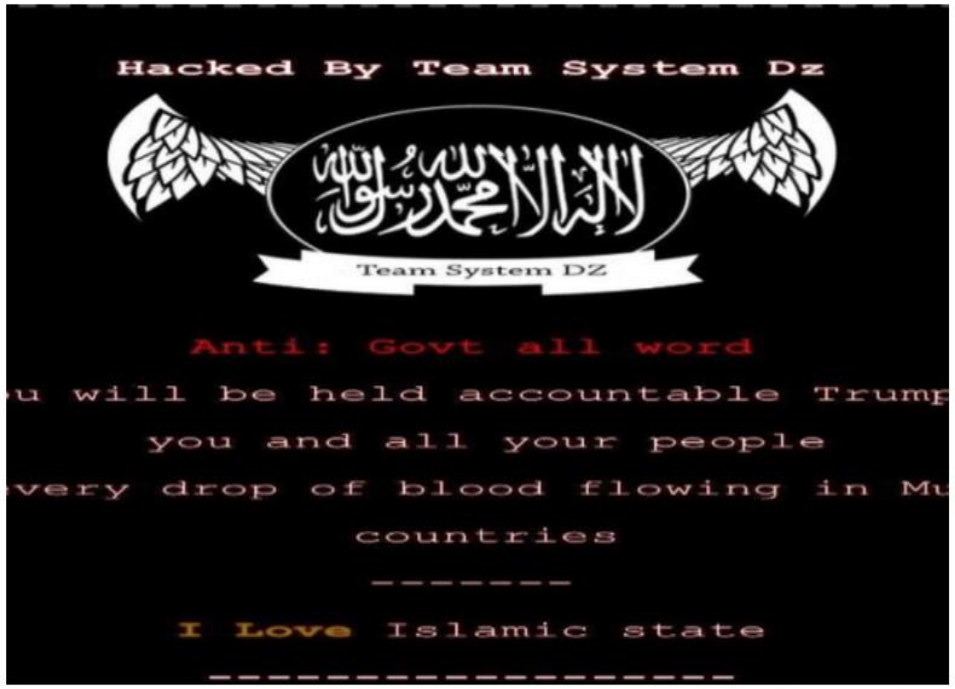
Homeland Security

31°

Sign In | Subscribe

The News&Observer

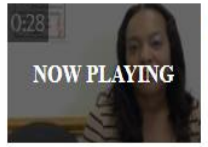
FULL MENU LOCAL NEWS SPORTS LIVING CLASSIFIEDS



North Carolina's elections board provided this image to state lawmakers in a December 2017 presentation. . - State Board of Elections and Ethics Enforcement

VIDEOS

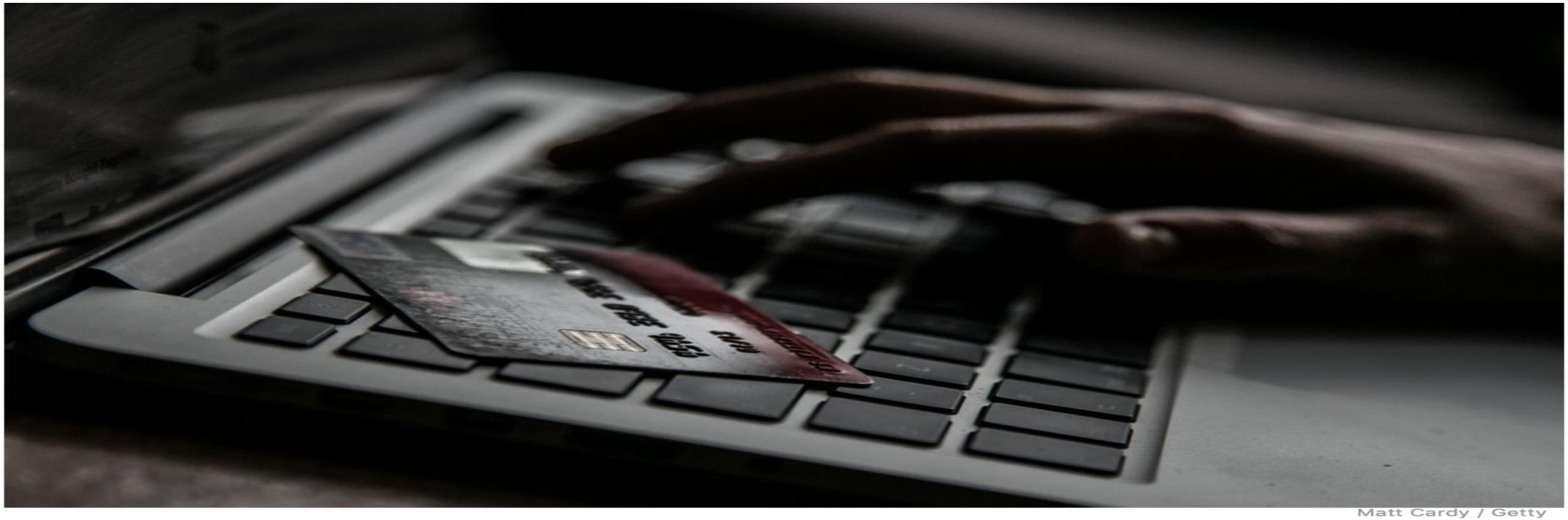
Can food stamps cover the costs of a healthy diet



Can food stamps cover the costs of a healthy diet

Senate leader Phil Berger discusses jail deaths

Homeland Security



Matt Cardy / Getty

A Cybersecurity Breach at Equifax Left Pretty Much Everyone's Financial Data Vulnerable

For Americans who want to protect their personal information, there is no way, in our current system, to do so.

GILLIAN B. WHITE | SEP 7, 2017 | BUSINESS

0.
0

Homeland Security

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN
Updated 3:00 PM ET, Wed March 28, 2018

Source: WSB

Atlanta mayor: Ransomware an attack on us all 01:38

City of Atlanta Needs $9.5 Million More for Ransomware Recovery

Posted by **Kevin Raske**

According to **multiple sources**, the City of Atlanta will need to find another $9.5 million to recover from the **"SamSam" ransomware attack which brought their city government to a grinding halt**. The number of applications and government services impacted by the attack has been revealed to be far greater than originally estimated, with the attack even affecting applications of the city police department and court system.

Homeland Security

America avoided election hacking in 2018. But are we ready for 2020?

By CHRIS GOOD Jan 18, 2019, 12:28 PM ET

Share Tweet

WATCH | Putin denies involvement in 2016 election hacking

Homeland Security

Progress in the 2018 Election Cycle

Establishment of the EI-ISAC

- In Feb. 18, the GCC adopted/ established the Elections Infrastructure ISAC – the fastest growing ISAC, ever

Funding Consideration Document

- In May, the GCC released a guidance document with potential short- and long-term funding considerations to support peers making decisions for election funding

Communications Protocols

- In July, the GCC issued a set of voluntary Communications Protocols to improve the efficiency and effectiveness of information sharing between Election Information Stakeholders

New Trainings and New Assessments

- Led by feedback from election officials, DHS now offers online "IT Management Training for Election Officials" and Remote Penetration Testing

National-level Election Security Tabletop Exercise

- In Aug., DHS hosted a three day tabletop exercise with 44 states and DC, 10 Federal agencies

Classified Briefings

- Classified information was able to be shared on several occasions, pushing more threat information to this sector than ever before

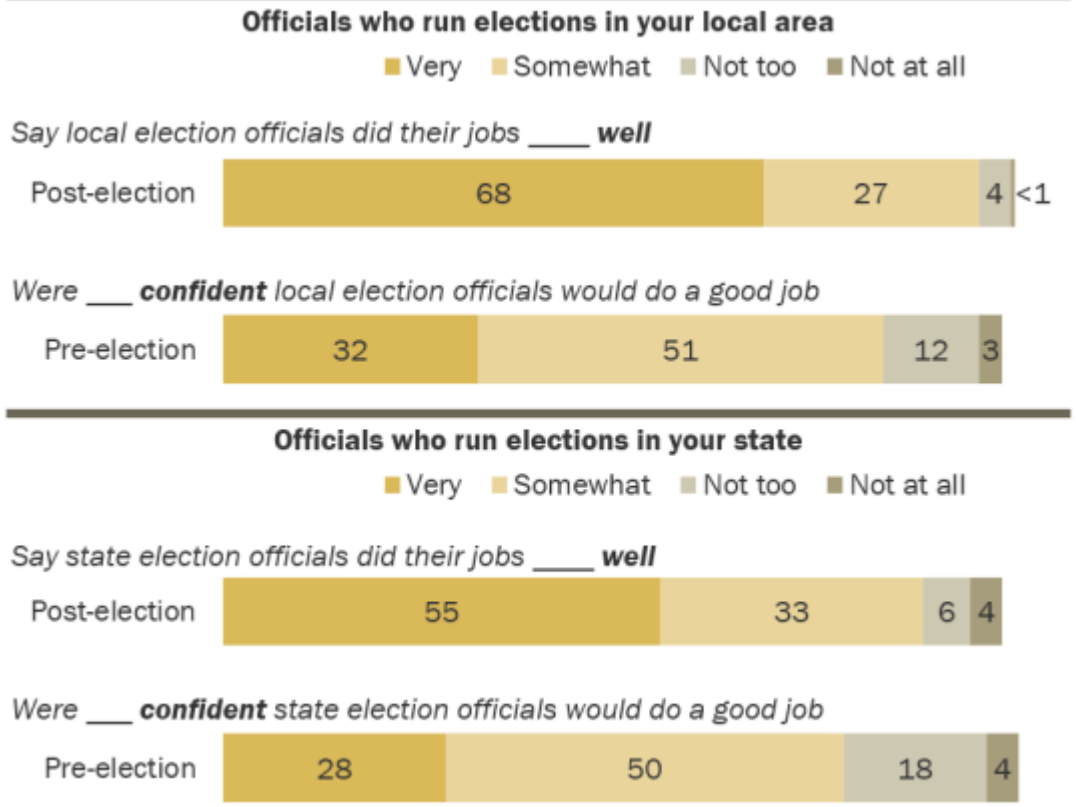
Election Situation Room

- On Election Day, DHS hosted the National Cybersecurity Situational Awareness Room. This online portal for state and local election officials and vendors facilitated rapid information sharing and gave election officials virtual access to the 24/7 operational watch floor of the NCCIC.

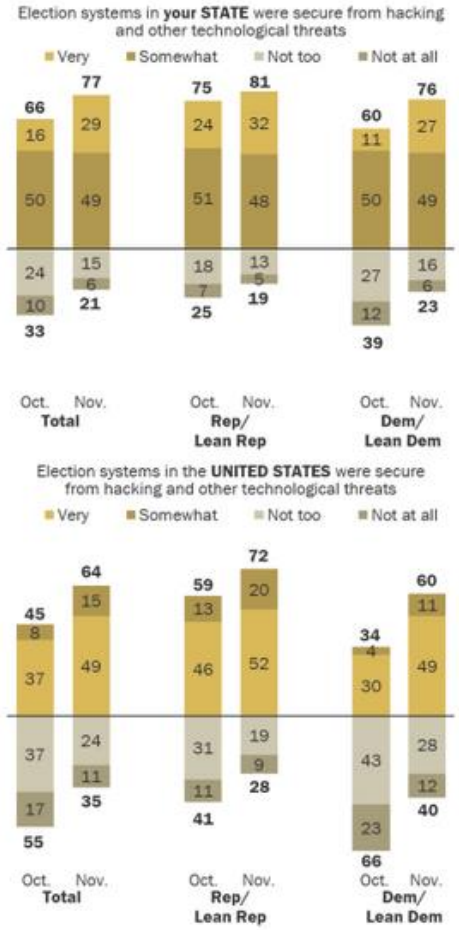
Homeland Security

Pew Research Center Report – Post 2018 Midterms

Large majorities say local election officials and poll workers did a good job in the 2018 election



Confidence in election systems' security rises, particularly among Democrats



Homeland Security

Election Infrastructure Security – Adoption of Services

SERVICE	Total
Cyber Resilience Review (CRR)	23
External Dependencies Management Assessment	17
Cyber Infrastructure Survey (CIS)	19
Cyber Hygiene Scanning (CyHy)	143
Hunt	25
Risk and Vulnerability Assessment (RVA)	36
Risk Penetration Testing (RPT)	11
Phishing Campaign Assessment (PCA)	10
Exercises	24

- 43 States have accepted at least one DHS Cybersecurity Service for EI
- 27 States have utilized at least two DHS Cybersecurity Services for EI
- 14 states have utilized three or more DHS Cybersecurity Services for EI
- Three states leveraged six or more DHS assessments for EI

Homeland Security

Top Recommendations Provided Across All EI Assessments

Mitigate Internet Vulnerabilities in a timely manner

- Recommend that EI Subsector entity managers mitigate all internet-accessible high and critical severity level vulnerabilities within 30 days. Vulnerabilities with lower severity levels should be reviewed and either mitigated, or the associated risk formally accepted, within 60 days.

Strengthen Password Policy and Auditing Processes

- Recommend the use of multi-factor password technology. Entities should perform regular audits of their password policy. Password best practices include ensuring that default passwords are never used in production, that strong passwords are required and used, and that administrators use encrypted password vaults.

Implement Network Segmentation

- Internal network architecture should protect and control access to the entity's most sensitive systems. Recommend that user workstations should be less trusted and connections to external networks should be isolated, controlled, and monitored.

Follow Cybersecurity Best Practices

- EI Subsector entities should follow established enterprise network best practices for IT infrastructure, including the implementation of a strong patching methodology for operating systems and third-party products.

Replace Unmaintainable Equipment

- All EI Subsector equipment should be maintainable with current security patching. Exceptions should be minimized and isolated.

DHS Positive Relationships – By the Numbers

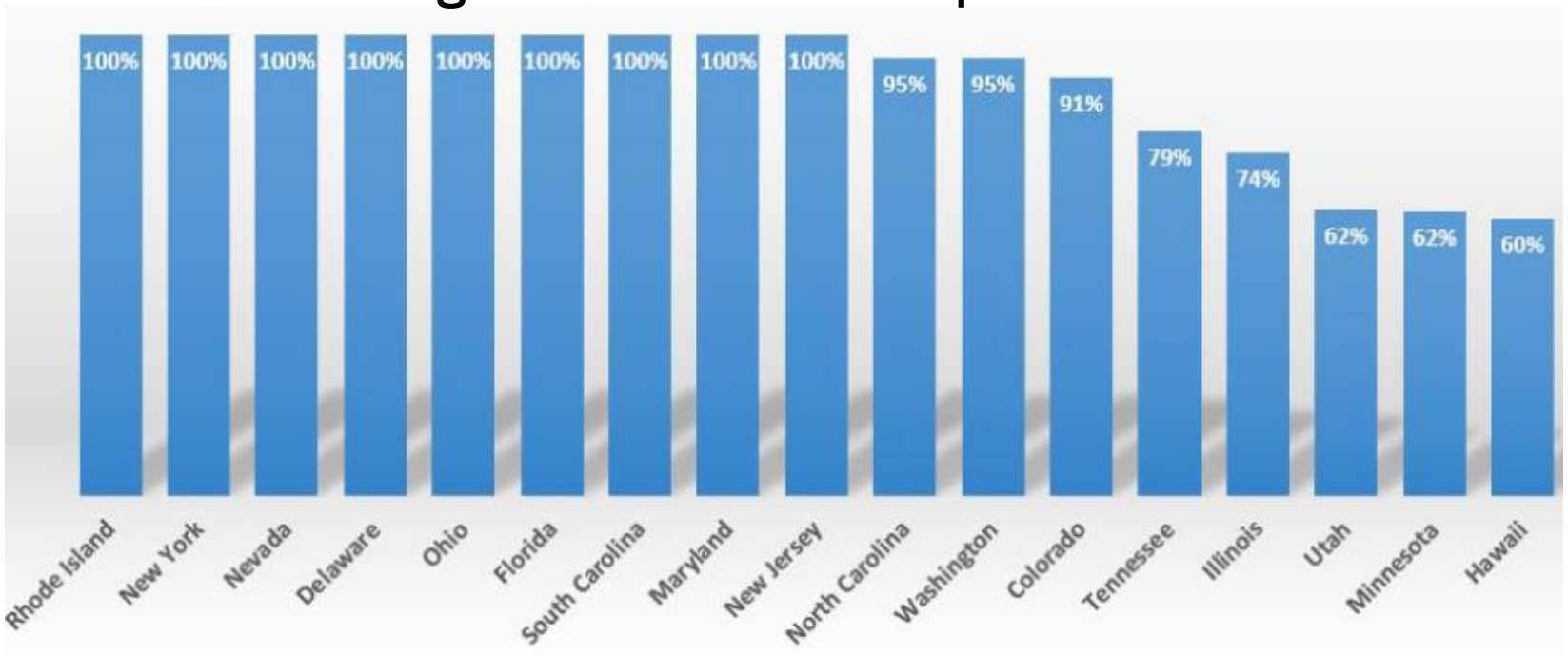
EI-ISAC:

- All 50 states and 4 territories
- 1400 election offices representing

Albert Sensors:

- 46 states have deployed Albert Sensors
- 20 existing statewide sensors
- 26 independent elections sensors
- 90 counties

States with High EI-ISAC Membership at the Local Level:



Homeland Security

CISA Cybersecurity 101

Christopher Krebs
Director, CISA
Department of Homeland Security
Christopher.Krebs@hq.dhs.gov

Matt Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Matthew.Masterson@hq.dhs.gov

Geoff Hale
Director, ETF
Department of Homeland Security
Geoffrey.Hale@hq.dhs.gov

Homeland Security