



MS-ISAC

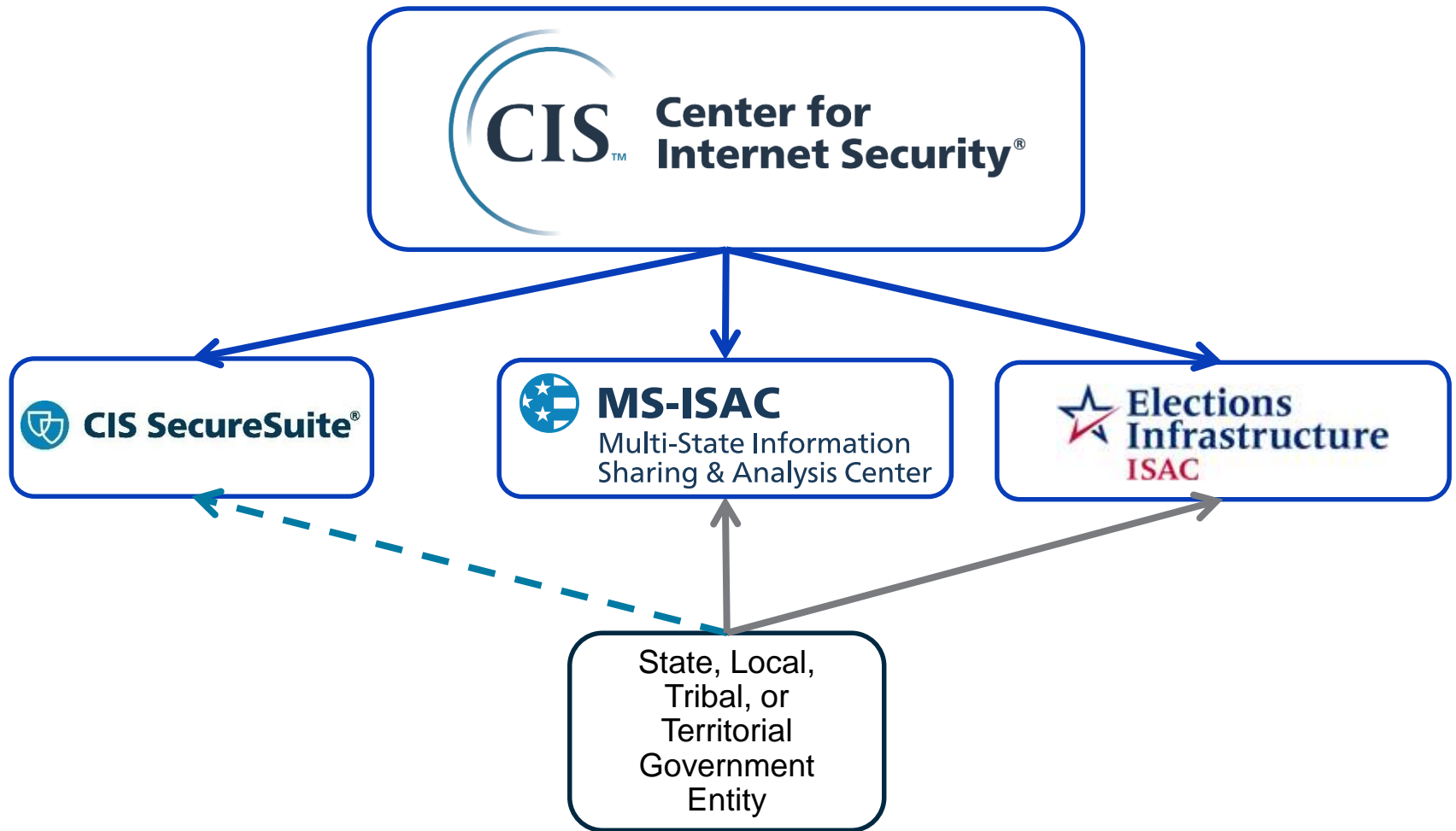
Multi-State Information
Sharing & Analysis Center

EI-ISAC Services

Federally Funded Cybersecurity
Resources for Elections Organizations

Eugene Kipniss

April 27, 2018



A Tale of Two ISACs

- **2003** – The MS-ISAC is founded as an initiative as part of New York State government for Northeast States
- **2004** – DHS funds the MS-ISAC as an initiative to support the cybersecurity needs of all State governments
- **2010** – The MS-ISAC breaks away from NYS and joins the Center for Internet Security as a program area

A Tale of Two ISACs

- **Summer 2016**
 - Public reporting of voter registration compromises
- **January 2017**
 - Intelligence Community Assessment (attribution of all elections related activity)
 - Critical Infrastructure Designation
- **July 2017**
 - Election Critical Infrastructure Working Group meets at MS-ISAC HQ

A Tale of Two ISACs

- **September 2017**
 - Election Infrastructure Subsector Government Coordinating Council (EIS-GCC) established
 - MS-ISAC Pilot for Elections Approved
- **October 2017-February 2018**
 - MS-ISAC Pilot for Elections (NJ, VA, IN, TX, CO, UT, WA)
- **February 2018**
 - EIS-GCC votes to establish EI-ISAC
- **March 2018**
 - EI-ISAC Official Launch

Who We Serve

EI-ISAC Members include:

- 47 State Elections Entities
- Over 450 Local Government Elections Entities

*County Clerks, Secretaries of State, Registrars of Voters,
Departments of Elections, Boards of Elections*

MS-ISAC Members Include:

State, Local, Tribal, and Territorial

*Cities, counties, towns, airports, public education, police
departments, ports, transit associations, and more*

About EI-ISAC Membership

Free and Voluntary
No Mandated Information Sharing
Registration is the only requirement!

To join or get more information:
<https://learn.cisecurity.org/ei-isac-registration>

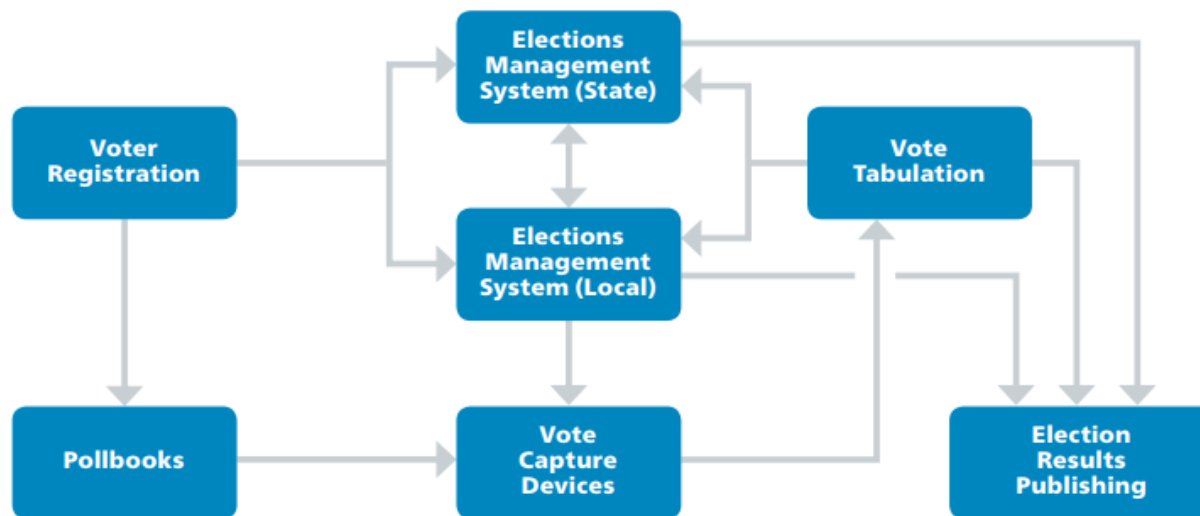
Why Government?

Criminals and Nation State threats look for data...
and governments have a lot of it!



Elections Systems

- Network Connected Systems and Components
- Indirectly Connected Systems
- Non-digital Elections Components



Transmission between components creates vulnerabilities

Potential Cybersecurity Risks

	Voter Registration	E- Pollbooks	Vote Capture	Vote Tabulation	Election Night Reporting
Misconfiguration					
SQL Injection					
Phishing					
Defacement					
Malware					
Man-in-the-Middle					
DDoS Attack					

Intelligence Sources

- 24x7 monitoring
- Analysis of more than 1 trillion logs/month
- Integration with federal agencies via the NCCIC
- Trusted private companies
- Constant contact with all ISACs



Information Sharing and Analysis Centers



MS-ISAC



Elections
Infrastructure
ISAC



FINANCIAL
SERVICES ISAC

EMR-ISAC



Real Estate
ISAC
Information Sharing
and Analysis Center
Serving the Commercial Facilities Sector



WaterISAC

REN-ISAC

R-CISC
RETAIL CYBER INTELLIGENCE SHARING CENTER



**HEALTHCARE
READY**
STRENGTHEN. SAFEGUARD. RESPOND.



IT ISAC



National Defense ISAC™

ONG-ISAC

DNG-ISAC



24 x 7 Security Operations Center

Central location to report any cybersecurity incident

- **Support:**
 - Network Monitoring Services
 - Research and Analysis
- **Analysis and Monitoring:**
 - Threats
 - Vulnerabilities
 - Attacks
- **Reporting:**
 - Cyber Alerts & Advisories
 - Web Defacements
 - Account Compromises
 - Hacktivist Notifications



To report an incident or request
assistance:

Phone: 1-866-787-4722

Email: soc@msisac.org



- 24x7x365 network monitoring
- Incident response and remediation
- Threat and vulnerability monitoring
- Election-specific threat intelligence
- Training sessions and webinars
- Promote security best practices
- DDoS mitigation and web protection services



Computer Emergency Response Team

- Incident Response (includes on-site assistance)
- Network & Web Application Vulnerability Assessments
- Malware Analysis
- Computer & Network Forensics
- Log Analysis
- Statistical Data Analysis
- Penetration Testing

To report an incident or request assistance:

Phone: 1-866-787-4722

Email: soc@msisac.org

- **MS-ISAC analysis to provide key context**
 - General election industry or election security reports
 - Legislative action on election security issues
 - Best practice examples from peers in the election community
 - General technology/cybersecurity stories that may have an election link/impact
- **Released on Wednesday afternoons**

TLP: WHITE
MS-ISAC Elections Pilot Weekly News Alert

TO: All MS-ISAC Elections Community Members

DATE: January 17, 2018

SUBJECT: Elections Pilot Weekly News Alert 1/17/18

The MS-ISAC Elections Pilot Weekly News Alert is a summary of open-source reporting on election security and topics that may be of interest to elections officials. The Weekly News Alert is intended to provide situational awareness of cyber risk landscape and cybersecurity best practices to election officials through open source news reporting and analysis by the MS-ISAC and other experts. If you would like to submit security-related stories that may be of interest to the elections community, please contact ben.spear@cisecurity.org.

Senate Bill Seeks Consequences for Future Election Interference - The Hill (1/16/18, 1/12/18)

On January 16, 2017, Senators Marco Rubio and Chris Van Hollen introduced the "Defending Elections from Threats by Establishing Redlines (DETER) Act," which lays out what specific activities to subvert U.S. elections would merit a federal response. The legislation would require the Administration to provide to Congress, within 90 days of enactment, plans to counter potential election interference from specific countries identified as a threat, and a notification to Congress of any foreign election interference within one month after every federal election. The bill also spells out specific penalties for future interference by Russia, such as a requirement to blacklist political figures and impose sanctions on Russia's finance, energy, and defense sectors.

MS-ISAC Analyst Note: The DETER Act acknowledges that nation-state actors are a persistent threat that will continue to target a range of U.S. interests and adds to the

- **Key Security Terms and Best Practices**
 - What it is
 - Why does it matter
 - What you can do
- **Released on Friday afternoons**

TLP: WHITE



Encryption

What it is: Encryption is the process whereby data is converted from a readable form (i.e., plaintext), to an encoded form (i.e., ciphertext). This encoding is designed to be unintelligible except by parties that possess a key to reverse the encoding process. This reversal process is called decryption. Data is encrypted using a mathematical algorithm that relies on passcodes (keys) that are typically randomly generated. The most trusted encryption algorithms are considered secure because they have been publicly available for years and have not been broken. An attack on data encrypted with a trusted encryption algorithm could take years for even the most powerful computers to break.

There are two types of encryption: asymmetric (public key) encryption and symmetric (private key) encryption.

	Asymmetric	Symmetric
Keys	2 keys – public (to be shared) and private (secret and possessed by only 1 person)	1 key – private (secret but shared between two or more partners)
Process	The sender encrypts information with recipient's public key and the recipient decrypts information with their private key	The sender encrypts information with a private key and the recipient decrypts information with the same private key
Speed	Slower	Faster

An easy way to understand these two types of encryption is two different types of lockboxes. In symmetric cryptography, you have a lockbox with one slot for a key. You make two copies of the key, and you give one to your friend. You lock the box with your copy, and when your friend comes along, they use their copy of the same key to unlock it.

Asymmetric cryptography is different. It's more like a deposit dropbox at a bank. The bank publishes the location of the dropbox (the public key), and once you drop your deposit into it, it's secure until the bank opens the box with the one and only copy of their key (the private key). Anyone can make a deposit once they know the location of the box, but only the bank can get deposits out.

Why does it matter: Encryption allows for the confidential storage and transmission of data, as well as proof that it originated with the person who claims to have sent it. Encrypting personally identifiable information (PII) with good encryption algorithms protects the data from accidental disclosure in the case of a data breach or malware infection. Elections offices may maintain a number of systems that utilize encryption and are responsible for identifying data that should be encrypted. This may

- Compiles analysis of elections-specific events identified by/reported to MS-ISAC
- Provides highlights of MS-ISAC election activities

TLP: AMBER



Elections Sector Quarterly Report

(MMMM DD, 2018 – Q4'17)

Table of Contents

Executive Overview	1
Monitoring Analysis	1
Incident Analysis	1
Election-Specific Products Disseminated	1
Other Key Products	2
Top News of the Quarter	2
Recent MS-ISAC Elections Speaking Engagements	2
New MS-ISAC Elections Members	2

Executive Overview

Actionable Notifications Q4 2017: xxx (% change)
Actionable Notifications YTD: xxx (% change)
Incident Notifications Q4 2017: (% change)
Incident Notifications YTD: xxx (% change)
Election Specific Products Disseminated: 9
Other Products Disseminated: 3
New State Election Agency Members: 10
New Local Election Agency Members: 14

Monitoring Analysis

Among the elections community, MS-ISAC monitored devices identified xxx actionable notifications in Q3 2017, which increased by xx% to xxx actionable notifications in Q4 2017. There was a year-over-year increase of xx%. This increase is attributed to...

TLP: WHITE

Election-specific Cyber Alerts

- **Short e-mail alerts regarding immediate threats**
 - Targeted at both executive and technical staff
- **Provides overview of activity and actionable recommendations**
 - Executive Overview
 - Executive Recommendations
 - Technical Overview
 - Technical Recommendations

TLP: **AMBER**

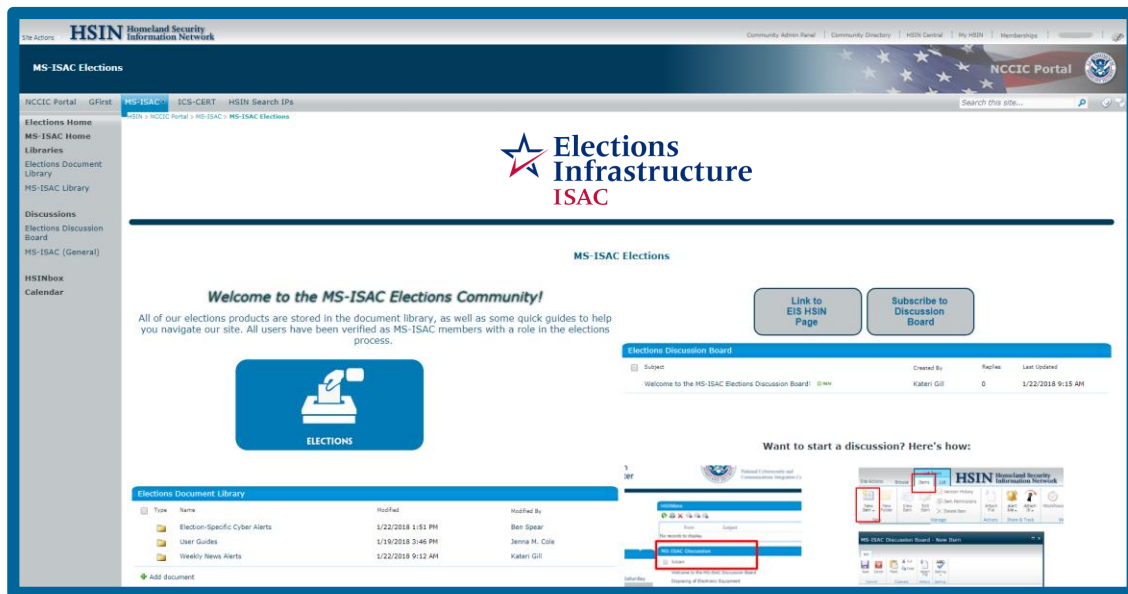
MS-ISAC ELECTIONS PILOT CYBER ALERT

TO: MS-ISAC Elections Pilot Participants

TLP: WHITE

Access to:

- MS-ISAC Cyber Alert Map
- Guides and templates
- Archived webcasts & products
- Elections sector message boards
- Table top exercises




Distributed in template form to allow for re-branding and redistribution by your agency




March, 2017
Volume 12, Issue 3

Common IT Wisdom That Keeps You Secure

**MS-ISAC**
Multi-State Information
Sharing & Analysis Center

*Insert your agency name and contact info
here*



From the Desk of Thomas F. Duffy, Chair, MS-ISAC

Day in and day out, employees hear the same things from their IT staff about cybersecurity and safety. Though they may sound like a broken record, there are very important reasons and rationale behind these practices and advice. Keeping safe and secure while connected isn't just about how your system is set up - it is also very much about how you end up using it. Below, we discuss some common IT staff wisdom and provide some background information and the rationale as to why it definitely merits your attention.

Make sure you lock your screen when you are away from your desk.

Screen locking policies exist for a reason. Even if you are leaving for just a few minutes at a time, be sure to lock your screen. Though physical intruders are rare during daytime and in conventionally secured offices, intrusions do occasionally happen. Screen locks also thwart opportunistic insider attacks from other employees that may seek to obtain information or access information beyond what they should normally have. If you don't adhere to a screen locking policy, an attacker can simply walk up and start manipulating or stealing your

Handbook for EI Security

- Intended for Elections Officials and Technical Support Teams
- Analyzes the risks of key election system components
- Describes specific technical controls and processes to improve security
- Assessment tool to be made available

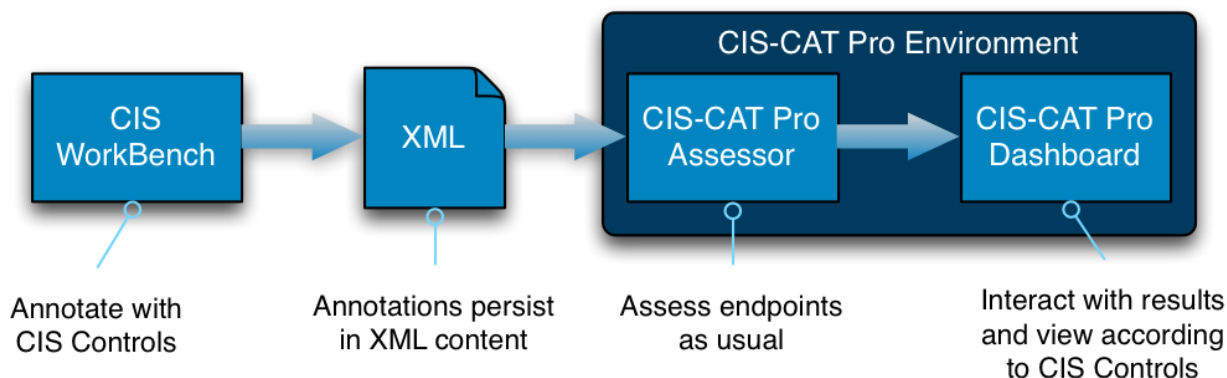


Order Hard Copies:

<https://learn.cisecurity.org/ei-handbook>

<https://www.cisecurity.org/elections-resources>

- **Controls**
 - Prioritized set of actions to protect your organization and data from known cyber attack vectors
- **Benchmarks**
 - Well-defined, un-biased, consensus-based industry best practices
- **Workbench**
 - Platform for creating and maintaining resources
 - <https://workbench.cisecurity.org>
- **CIS-CAT Pro**
 - Configuration and Vulnerability Assessment Tool
 - Assessor and Dashboard can be downloaded from Workbench



What Should I Do With This Info?

- Implement the recommendations
- Provide it to your IT staff
- Disseminate to your local distribution lists
- Post it to any portal you control



SHARE IT!!!!

TLP: WHITE

Google - Protect Your Election

- Project Shield DDoS Protection
- Two Factor Authentication
- Advanced Phishing Protection (GSuite)
- Password Alert Plugin for Chrome
- General Security Support

Protect Your Election



Cloudflare – Athenian Project

- Full enterprise offering
- DDoS protection
- Web Application Firewall (WAF)
- Content Delivery Network (CDN)
- 24x7 Support



Both services are available to any SLTT organization responsible for public-facing elections infrastructure related to voter registration information and election night reporting

An Elections-focused Cyber Defense Suite

- 24x7x365 network monitoring
- Incident response and remediation
- Threat and vulnerability monitoring
- Election-specific threat intelligence
- Training sessions and webinars
- Promote security best practices
- DDoS mitigation and web protection services





EI-ISAC 24x7 Security Operations Center

1-866-787-4722

SOC@cisecurity.org

ELECTIONS@CISEcurity.ORG

Eugene Kipniss
Senior Program Specialist, EI-ISAC
518.880.0716
Eugene.kipniss@cisecurity.org