MS-ISAC as the Elections ISAC

Ben Spear
Project Lead, EI-ISAC
Center for Internet Security

CIS is a forward-thinking, nonprofit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

**CIS Benchmarks™**
Consensus-based, internationally-recognized software configuration guidelines curated by experienced IT practitioners to help assess and improve network security.

**MS-ISAC™**
Multi-State Information Sharing & Analysis Center®
The focal point for cybersecurity resources for U.S. State, Local, Tribal, and Territorial (SLTT) governments. 24x7 Security Operations Center provides real-time monitoring, threat warnings, and incident response.

**CIS Controls**
A prioritized set of policy-level controls that set a secure foundation for organizations around the world. Common security practices distilled into a scalable, actionable list to provide real security for real threats.

**CIS Services**
Services such as vulnerability assessment, incident response, phishing exercises, and monitoring.

**CIS CyberMarket**
Purchasing program that serves SLTT governments and not-for-profit entities to improve cybersecurity through cost-effective group procurement.

TLP: WHITE
The MS-ISAC has been designated by DHS as the key resource for cyber threat prevention, protection, response and recovery for the nation’s state, local, tribal, and territorial governments.

https://www.cisecurity.org/ms-isac/
Members include:

- 50 State Governments
- 79 DHS-Recognized Fusion Centers
- 6 Territorial Governments
- 48 Tribal Governments
- More than 1,900 local governments

Over 200 state and local election agencies

State, Local, Tribal, and Territorial
Cities, counties, towns, airports, public education, police departments, ports, transit associations, and more

TLP: WHITE
MS-ISAC: Who We Work With

• Integration with federal agencies via the NCCIC
• Trusted private companies
• Constant contact with all ISACs
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
Network Monitoring (Albert)

- SLTT focus
- 24x7 research, analysis, and support
- Signatures unique to SLTT governments
- Integration of research on specific attacks and actors, including nation-state actors (APT)
- Real-time information sharing
- Experienced cybersecurity analysts who review each event minimizing the number of false-positive notifications
Monitoring of IP Ranges & Domains

**IP Monitoring**
- IPs connecting to sinkholed C2s
- Compromised IPs
- Indicators of compromise from MS-ISAC network monitoring

**Domain Monitoring**
- Notifications on compromised user credentials, open source, and third party information
- Vulnerability Management Program (VMP)

Send domains, IP ranges, and contact info to: soc@msisac.org
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
Elections Weekly News Alert

• 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

---

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@csisecurity.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
Elections Sector Quarterly Report

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

**Table of Contents**

**Executive Overview**
- Actionable Notifications Q4 2017: xxx (% change)
- Actionable Notifications YTD: xxx (% change)
- Incident Notifications Q4 2017: yyy (% change)
- Incident Notifications YTD: zzz (% 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...
HSIN Community of Interest

Access to:

- MS-ISAC Cyber Alert Map
- Archived webcasts & products
- Table top exercises
- Guides and templates
- Elections sector message boards
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
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
Or
ELECTIONS@CISSECURITY.ORG
SecureSuite

- **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](https://workbench.cisecurity.org)

- **CIS-CAT Pro**
  - Configuration and Vulnerability Assessment Tool
  - Assessor and Dashboard can be downloaded from Workbench
DDoS Mitigation and Web Protection Services

Google - Protect Your Election
  • Project Shield DDoS Protection
  • Two Factor Authentication
  • Advanced Phishing Protection (GSuite)
  • Password Alert Plugin for Chrome

Cloudflare – Athenian Project
  • Full enterprise offering
  • DDoS protection
  • Web Application Firewall (WAF)
  • Content Delivery Network (CDN)

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
• DDoS mitigation and web protection services
• Election-specific threat intelligence
• Training sessions and webinars
• Promote security best practices
How do I become a member?

Free and Voluntary
No Mandated Information Sharing

1. Visit and complete our registration form
2. Agree to the Terms and Conditions
3. Receive a “Welcome” Email
4. Provide contact details for key staff
5. Start receiving notifications and products
6. Attend a new member webcast

https://learn.cisecurity.org/ei-isac-registration
EI-ISAC 24x7 Security Operations Center
1-866-787-4722
SOC@cisecurity.org

ELECTIONS@CISECURITY.ORG

Ben Spear
Project Lead, EI-ISAC
518.880.0705
ben.spear@cisecurity.org