2021 Nationwide Cybersecurity Review

Elections Peer Group

23 State and 77 Local Participant Organizations

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

Elections Infrastructure ISAC®

Elections Peer Groups

State and Local Elections Participants

The MS-ISAC measured the areas of highest and lowest cybersecurity maturity, as reported from the 2021 Nationwide Cybersecurity Review (NCSR) assessment. This resource is based on the data from the 2021 NCSR, which was open for data collection between 10/1/2021 and 2/28/2022. It is our aim to call attention to these areas of interest and, even more important, to call attention to resources, guidance, and services that may serve to increase the maturity of those lowest-scoring areas. To better inform the community of where to direct activity and resources for cybersecurity maturity, it is crucial we increase elections participation in the NCSR to get a more representative view of the community's cybersecurity trends. This document is based on aggregated data from all organizations in this peer group and may not illustrate one specific organization's particular areas of lowest maturity. We recommend each individual organization use this guidance by taking the following steps:

1. Determine your lowest-scoring NIST Cybersecurity Framework (CSF) categories based on your NCSR scores. Start by logging in to the NCSR platform and reviewing your organization's results in the "Report Portal." The report named "Current NCSR Results–Detail View" is a good starting point. Utilize the NCSR General User Guide to navigate to this reporting"
2. Leverage this document to determine if your lowest scoring areas align with those of your peer group reported below.
3. Consult the MS-ISAC Cybersecurity Resources Guide or the report titled "Cybersecurity Resources & NCSR Results Mapping" in the NCSR platform to see what no-cost resources are available".
4. Note, all resources and reporting do not need to be used at once. This document is meant to help prioritize an organization's findings and plan cybersecurity improvements.

Findings

The MS-ISAC also looked into how both State Elections and Local Elections scored against their non-elections State and Local counterparts. An important note to consider for these comparisons is that both the State Elections and Local Elections peer groups are significantly smaller than their overall State and Local counterparts. The tables below highlight the highest and lowest scoring NIST CSF categories for both State and Local Elections.

2021 State Elections Peer Group

Highest Maturity Level NIST CSF Categories	Lowest Maturity Level NIST CSF Categories
Protect: Awareness and Training	**Identify:** Supply Chain Risk Management
Protect: Identity Mgmt. and Access Control	**Identify:** Risk Management Strategy
Respond: Mitigation	**Identify:** Asset Management
Recover: Recovery Planning	**Identify:** Governance
Recover: Communications	**Respond:** Response Planning

2021 Local Elections Peer Group

Highest Maturity Level NIST CSF Categories	Lowest Maturity Level NIST CSF Categories
Protect: Identity Mgmt. and Access Control	**Identify:** Supply Chain Risk Management
Protect: Awareness and Training	**Identify:** Risk Management Strategy
Protect: Protective Technology	**Respond:** Improvements
Detect: Security Continuous Monitoring	**Recover:** Improvements
Protect: Data Security	**Recover:** Communications

For additional information on this NCSR Snapshot or the NCSR overall, please contact NCSR@cisecurity.org.

The following resources are available to assist with the lower-scoring categories of both the State and Local Elections Peer Groups. The MS-ISAC recommends evaluating the lowest scoring activities that are most applicable to your organization. Once you have identified these activities, you can begin creating a cybersecurity roadmap for improvement.

Identify: Supply Chain Risk Management

MS-ISAC Developed Policy Templates

- Identification and Authentication Policy
- Security Assessment and Authorization Policy
- System and Services Acquisition Policy

CIS Developed Guides

While these guides are focused on the elections community, their principles can be applied within any organization.

- CIS Technology Procurement Guide
- Managing Cybersecurity Supply Chain Risks in Election Technology: A Guide for Election Technology Providers

MS-ISAC and Metrics Workgroup Developed Guide

- Supply Chain Cybersecurity Resources Guide

Federal Guidance

- DHS CISA Supply Chain Risk Management Guidance

Identify: Risk Management Strategy

MS-ISAC Developed Policy Template

- Information Security Policy
- Information Security Risk Management Standard
- Risk Assessment Policy

Identify: Asset Management

MS-ISAC Developed Policy Templates

- Acceptable Use of Information Technology Resource Policy
- Access Control Policy
- Account Management/Access Control Standard
- Identification and Authentication Policy
- Information Security Policy
- Security Assessment and Authorization Policy
- Security Awareness and Training Policy
- CIS Hardware and Software Asset Tracking Spreadsheet: This free spreadsheet is created by CIS to help track enterprise systems and other assets. It can be modified as needed to meet an enterprise's unique needs. The primary elements within the spreadsheet are also described within the relevant appendix.

Open Source Resources and Tools

Descriptions courtesy of the CIS "Microsoft Windows 10 Cyber Hygiene Guide":

- Nmap: Famous multipurpose network scanner, used by system administrators and hackers across the world to identify which devices are connected to a network. Be careful to only scan networks for which permission was explicitly given. It is often impolite, and in many cases illegal, to scan networks owned by others.
- ZenMap: This tool builds on top of Nmap, and puts a graphic user interface on top of it to make the tool easier to use for those who do not feel comfortable using the command line.
- Spiceworks: This is a free IT inventory and asset management software to identify devices and software on a network.
- Netwrix: Variety of free tools to identify information about administrative access on any relevant systems.
- OpenAudIT: Inventory applications and software on workstation servers and network devices.

Additional Open Source Tools

- OpenVAS
- SnipeIT
- Draw.io

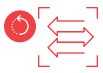
Identify: Governance

MS-ISAC Resource Guide and Service

- MS-ISAC Risk Assessment Guide
- Malicious Domain Blocking and Reporting (MDBR)

Additional Open Source Tool

- Eramba GRC



Respond: Response Planning

MS-ISAC Developed Policy Templates

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy
- Planning Policy

Additional Open Source Tool

- The Hive

Recover: Communications

MS-ISAC Developed Policy Templates

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy

Respond: Improvements

Recover: Improvements

MS-ISAC Developed Policy Templates

- Computer Security Threat Response Policy
- Contingency Planning Policy
- Cyber Incident Response Standard
- Incident Response Policy

MS-ISAC Business Resiliency Workgroup Resources

Contact info@cisecurity.org for access to the resources:

- Incident Response Plan Templates
- After Action Report Templates
- "Lessons Learned" Guidance
- Incident Response & Disaster Recovery Table Top Exercises

Data Backup Tools and Resources (descriptions courtesy of the CIS "Microsoft Windows 10 Cyber Hygiene Guide")

- Microsoft Backup and Restore: A backup utility tool installed on Microsoft operating systems.
- EaseUS: This free program can be configured to take system images.
- Amanda Network Backup: Free, open source backup tool.
- Bacula: Open source network backup and recovery solution.
- Carnegie Mellon: The university makes their Incident Response Plan available, that can be used as a resource for others.
- State of Oregon: The Oregon State Government provides a template for an Incident Response Plan.

Additional Information

Nationwide Cybersecurity Review (NCSR) Webpage

Information on the no-cost, annual self-assessment from the MS-ISAC, as well as associated resources, is available on this page.

Full CIS "Microsoft Windows 10 Cyber Hygiene Guide"

A number of the listed resources are included within this guide, courtesy of the CIS Controls team.

CIS SecureSuite Membership

All state, local, tribal, and territorial organizations can access CIS SecureSuite membership at no cost. This includes the CIS Controls, the CIS Benchmarks, and CIS-CAT Pro Assessor for an automated comparison of your configurations against CIS secure configuration Benchmarks. The CIS Controls provide security best practices along with guidance on how to prioritize the controls, known as the CIS Implementation Groups (IGs). The CIS Benchmarks were created from the global community of cybersecurity experts and have more than 100 configuration guidelines to safeguard systems against today's evolving cyber threats. The CIS-CAT Pro combines the security guidance of the CIS Controls and CIS Benchmarks into a single assessment tool.

Federal Virtual Training Environment (FedVTE) No-Cost Online Training

Registration and course information.

No or Low-cost CIS & MS-ISAC Services

Relevant services include Albert Network Monitoring and Management, CIS Endpoint Security Services (ESS), and Malicious Domain Blocking and Reporting (MDBR)