

2021

Nationwide Cybersecurity Review

**Snapshot of Lowest Scoring Categories—
All Peer Groups**

3,267 Total Participant Organizations



Lowest Scoring Categories

The Nationwide Cybersecurity Review (NCSR) is a baseline assessment that can help U.S. State, Local, Tribal, and Territorial (SLTT) governments measure their cybersecurity maturity. This document reviews the 10 lowest scoring NCSR categories reported across all peer groups, as identified within the 2021 NCSR results. The 2021 NCSR was open for data collection between 10/01/2021 and 2/28/2022. It is our aim to call attention to these areas of interest, and most importantly, to call attention to resources, guidance, and services that may serve to increase the maturity of those lowest-scoring areas. 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 an individual organization use this guidance in 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 across the SLTT community reported below, or if you scored relatively low on the 7-point NCSR maturity scale in other areas.
- 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.

**2021 Lowest Maturity Level
NIST CSF Categories – All Peer
Groups**

Identify: Supply Chain Risk Management

Identify: Risk Management Strategy

Identify: Asset Management

Protect: Information Protection Processes and Procedures

Protect: Data Security

Detect: Detection Processes

Respond: Improvements

Recover: Recovery Planning

Recover: Communications

Recover: Improvements

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:



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](#)
- [A Guide for Ensuring Security in Election Technology Procurements](#)

MS-ISAC and Metrics Working Group Developed Guide

- [Supply Chain Cybersecurity Resources Guide](#)

Federal Guidance

- [DHS CISA Supply Chain Risk Management Guidance](#)



Identify: Risk Management Strategy

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](#).



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



Protect: Information Protection Processes and Procedures

MS-ISAC Developed Policy Templates

- Access Control Policy
- Account Management/Access Control Standard
- Authentication Tokens Standard
- Configuration Management Policy
- Identification and Authentication Policy
- Sanitization Secure Disposal Standard
- Secure Configuration Standard
- Secure System Development Life Cycle Standard



Protect: Data Security

MS-ISAC Developed Policy Templates

- Access Control Policy
- Account Management/Access Control Standard
- Authentication Tokens Standard
- Configuration Management Standard
- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Encryption Standard
- Identification and Authentication Policy
- Incident Response Policy
- Information Security Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Patch Management Standard
- Sanitization Secure Disposal Standard
- Secure Configuration Standard
- Secure System Development Life Cycle Standard

Open Source Tools

- [Open DLP](#)
- [Tripwire](#)
- [AIDE](#)
- [Agnito](#)
- [W2AF](#)
- [Wapiti](#)



Detect: Detection Processes

MS-ISAC Developed Policy Templates

- [Computer Security Threat Response Policy](#)
- [Information Security Risk Management Standard](#)
- [Cyber Incident Response Standard](#)
- [Incident Response Policy](#)



Respond: Improvements

MS-ISAC Developed Policy Templates

- [Computer Security Threat Response 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 & 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](#).



Recover: Recovery Planning

MS-ISAC Developed Policy Templates

- [Computer Security Threat Response Policy](#)
- [Contingency Planning Policy](#)
- [Cyber Incident Response Standard](#)
- [Incident Response Policy](#)



Recover: Communications

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](#)



Recover: Improvements

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 \(MDBR\)](#)

