2020 Nationwide Cybersecurity Review

Public Utilities Peer Group

21 Participant Organizations

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

Elections Infrastructure ISAC®

Public Utilities Peer Group

The MS-ISAC measured the areas of highest and lowest cybersecurity maturity, as reported from the 2020 Nationwide Cybersecurity Review (NCSR) assessment. This resource is based on the data from the 2020 NCSR, which was open for data collection between 10/1/2020 and 2/28/2021. 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. The public utilities subsector had a total of 21 organizations that completed the assessment. 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.
2. Leverage this document to determine if your lowest areas align with those of your peer group reported below, or if you scored relatively low on the 7-point NCSR maturity scale in other areas.
3. Leverage resources and guidance listed below for those lowest-scoring areas that may need improvement in your organization.
4. Consult the Cybersecurity Resources Guide to see what no-cost courses are available. This includes professional development on the DHS FedVTE training platform that is accessible to SLTT organizations.

MS-ISAC Developed Resources

- Cybersecurity Resources Guide
- NCSR Resources Guide Mapping Template
- NCSR Mapping Template to CIS Controls
- First Steps Within a Cybersecurity Program

2020 PUBLIC UTILITIES PEER GROUP	
Highest Maturity Level NIST CSF Categories	**Lowest Maturity Level NIST CSF Categories**
Protect: Identity Management and Access Control	**Identify:** Supply Chain Risk Management
Protect: Awareness and Training	**Identify:** Risk Management Strategy
Protect: Maintenance	**Identify:** Governance
Identify: Business Environment	**Respond:** Improvements
Detect: Continuous Monitoring	**Recover:** Improvements

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

The following resources are available to assist with the lower-scoring categories of the Public Utilities Peer Group overall:

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

FedVTE Courses:

The Election Official as IT Manager; Cyber Risk Management for Managers; ISACA Certified Information Security Manager (CISM) Prep; (ISC)2 (TM) CAP Certification Prep Self Study 2014; Cybersecurity Overview for Managers; CompTIA Advanced Security Practitioner; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018

Identify: Governance

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.

Additional Open Source Tools:

- OpenVAS
- Eramba GRC

FedVTE Courses:

ISACA Certified Information Security Manager (CISM) Prep; (ISC)2 (TM) CAP Certification Prep Self Study 2014; Cybersecurity Overview for Managers; Emerging Cybersecurity Threats; (ISC)2 (TM) CISSP (R) Certification Prep 2018; (ISC)2 (TM) CISSP Concentration: ISSEP Prep; (ISC)2 (TM) CISSP: ISSMP Prep 2018; Cyber Risk Management for Managers; 101–Critical Infrastructure Protection; 101 Reverse Engineering; CompTIA Advanced Security Practitioner

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@msisac.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: 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@msisac.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.

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

Registration and course information available on this page.