NIST Cybersecurity Framework

Policy Template Guide

Center for Internet Security®

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

Contents

Introduction

The Multi-State Information Sharing & Analysis Center (MS-ISAC) is offering this guide to participants of the Nationwide Cybersecurity Review (NCSR) and MSISAC members, as a resource to assist with the application and advancement of cybersecurity policies.

The policy templates are provided courtesy of the State of New York and the State of California. The templates can be customized and used as an outline of an organizational policy, with additional details to be added by the end user.

The NCSR question set represents the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). This guide gives the correlation between 49 of the NIST CSF subcategories, and applicable policy and standard templates. A NIST subcategory is represented by text, such as "ID.AM-5." This represents the NIST function of Identify and the category of Asset Management.

For additional information on services provided by the Multi-State Information Sharing & Analysis Center (MS-ISAC), please refer to the following page: https:// www.cisecurity.org/ms-isac/services/. These policy templates are also mapped to the resources MS-ISAC and CIS provide, open source resources, and free FedVTE training: https://www.cisecurity.org/wp-content/uploads/2019/11/CybersecurityResources-Guide.pdf.

Disclaimer: These policies may not reference the most recent applicable NIST revision, however may be used as a baseline template for end users. These policy templates are not to be used for profit or monetary gain by any organization.

NIST FUNCTION:

Govern

Govern: Organizational Context (GV.OC)

GV.OC-01 The organizational mission is understood and informs cybersecurity risk management

- Information Security Policy

GV.OC-02 Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered

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

GV.OC-03 Legal, regulatory, and contractual requirements regarding cybersecurity—including privacy and civil liberties obligations—are understood and managed

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

GV.OC-04 Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated

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

GV.OC-05 Critical objectives, capabilities, and services that stakeholders depend on or expect from the organization are understood and communicated

- System and Communications Protection Policy
- Information Classification Standard
- Information Security Policy

Govern: Risk Management Strategy (GV.RM)

GV.RM-01 Risk management objectives are established and agreed to by organizational stakeholders

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

GV.RM-02 Risk appetite and risk tolerance statements are established, communicated, and maintained

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

GV.RM-03 Cybersecurity risk management activities and outcomes are included in enterprise risk management processes

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

GV.RM-04 Strategic direction that describes appropriate risk response options is established and communicated

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

GV.RM-05 Lines of communication across the organization are established for cybersecurity risks, including risks from suppliers and other third parties

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

GV.RM-06 A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated

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

GV.RM-07 **Strategic opportunities (i.e., positive risks) are characterized and are included in organizational cybersecurity risk discussions**

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

Govern: Roles, Responsibilities, and Authorities (GV.RR)

GV.RR-01 **Organizational leadership is responsible and accountable for cybersecurity risk and fosters a culture that is risk-aware, ethical, and continually improving**

- Acceptable Use of Information Technology Resource Policy
- Information Security Policy
- Security Awareness and Training Policy

GV.RR-02 **Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced**

- Acceptable Use of Information Technology Resource Policy
- Information Security Policy
- Security Awareness and Training Policy

GV.RR-03 **Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies**

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

GV.RR-04 **Cybersecurity is included in human resources practices**

- Information Security Policy
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Security Awareness and Training Policy

Govern: Policy (GV.PO)

GV.PO-01 **Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced**

- Personnel Security Policy
- Physical and Environmental Protection Policy
- Security Awareness and Training Policy

GV.PO-02 **Policy for managing cybersecurity risks is reviewed, updated, communicated, and enforced to reflect changes in requirements, threats, technology, and organizational mission**

- Personnel Security Policy
- Physical and Environmental Protection Policy
- Security Awareness and Training Policy

Govern: Oversight (GV.OV)

GV.OV-01 **Cybersecurity risk management strategy outcomes are reviewed to inform and adjust strategy and direction**

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

GV.OV-02 **The cybersecurity risk management strategy is reviewed and adjusted to ensure coverage of organizational requirements and risks**

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

GV.OV-03 **Organizational cybersecurity risk management performance is evaluated and reviewed for adjustments needed**

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

Govern: Cybersecurity Supply Chain Risk Management (GV.SC)

GV.SC-01 A cybersecurity supply chain risk management program, strategy, objectives, policies, and processes are established and agreed to by organizational stakeholders

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

GV.SC-02 Cybersecurity roles and responsibilities for suppliers, customers, and partners are established, communicated, and coordinated internally and externally

- Acceptable Use of Information Technology Resource Policy
- Information Security Policy
- Security Awareness and Training Policy

GV.SC-03 Cybersecurity supply chain risk management is integrated into cybersecurity and enterprise risk management, risk assessment, and improvement processes

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

GV.SC-04 Suppliers are known and prioritized by criticality

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

GV.SC-05 Requirements to address cybersecurity risks in supply chains are established, prioritized, and integrated into contracts and other types of agreements with suppliers and other relevant third parties

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

GV.SC-06 Planning and due diligence are performed to reduce risks before entering into formal supplier or other third-party relationships

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

GV.SC-07 **The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship**

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

GV.SC-08 **Relevant suppliers and other third parties are included in incident planning, response, and recovery activities**

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy
- Systems and Services Acquisition Policy

GV.SC-09 **Supply chain security practices are integrated into cybersecurity and enterprise risk management programs, and their performance is monitored throughout the technology product and service life cycle**

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

GV.SC-10 **Cybersecurity supply chain risk management plans include provisions for activities that occur after the conclusion of a partnership or service agreement**

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

NIST FUNCTION:

Identify

Identify: Asset Management (ID.AM)

ID.AM-1 **Inventories of hardware managed by the organization are maintained**

- 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

ID.AM-2 **Inventories of software, services, and systems managed by the organization are maintained**

- 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

ID.AM-3 **Representations of the organization's authorized network communication and internal and external network data flows are maintained**

- System and Communications Protection Policy

ID.AM-4 **Inventories of services provided by suppliers are maintained**

- System and Communications Protection Policy

ID.AM-5 **Assets are prioritized based on classification, criticality, resources, and impact on the mission**

- Information Classification Standard
- Information Security Policy

ID.AM-7 **Inventories of data and corresponding metadata for designated data types are maintained**

- Information Classification Standard
- Information Security Policy

ID.AM-8 **Systems, hardware, software, services, and data are managed throughout their life cycles**

- Access Control Policy
- Account Management/Access Control Standard
- Configuration Management Policy
- Identification and Authentication Policy
- Sanitization Secure Disposal Standard
- Secure Configuration Standard
- Secure System Development Life Cycle Standard
- Maintenance Policy
- Remote Access Standard
- Security Logging Standard

Identify: Risk Assessment (ID.RA)

ID.RA-01 **Vulnerabilities in assets are identified, validated, and recorded**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

ID.RA-02 **Cyber threat intelligence is received from information sharing forums and sources**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

ID.RA-03 **Internal and external threats to the organization are identified and recorded**

- Encryption Standard
- Information Security Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Security Assessment and Authorization Policy
- Vulnerability Scanning Standard
- Patch Management Standard

ID.RA-04 **Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

ID.RA-05 **Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization**

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

ID.RA-06 **Risk responses are chosen, prioritized, planned, tracked, and communicated**

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

ID.RA-07 **Changes and exceptions are managed, assessed for risk impact, recorded, and tracked**

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

ID.RA-08 **Processes for receiving, analyzing, and responding to vulnerability disclosures are established**

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

ID.RA-09 **The authenticity and integrity of hardware and software are assessed prior to acquisition and use**

- System and Information Integrity Policy

ID.RA-10 **Critical suppliers are assessed prior to acquisition**

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

Identify: Improvement (ID.IM)

ID.IM-01 **Improvements are identified from evaluations**

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

ID.IM-02 **Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties**

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

ID.IM-03 **Improvements are identified from execution of operational processes, procedures, and activities**

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

ID.IM-04 **Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved**

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy
- Systems and Services Acquisition Policy
- Contingency Planning Policy

NIST FUNCTION:

Protect

Protect: Identity Management and Access Control (PR.AA)

PR.AA-01 **Identities and credentials for authorized users, services, and hardware are managed by the organization**

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

PR.AA-02 **Identities are proofed and bound to credentials based on the context of interactions**

- Access Control Policy
- Account Management/Access Control Standard
- Authentication Tokens Standard
- Configuration Management Policy
- Identification and Authentication Policy

PR.AA-03 **Users, services, and hardware are authenticated**

- Remote Access Standard

PR.AA-04 **Identity assertions are protected, conveyed, and verified**

- Access Control Policy
- Account Management/Access Control Standard
- Authentication Tokens Standard
- Configuration Management Policy
- Identification and Authentication Policy

PR.AA-05 **Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties**

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

PR.AA-06 **Physical access to assets is managed, monitored, and enforced commensurate with risk**

- Encryption Standard
- Information Security Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- System and Communications Protection Policy

Protect: Awareness and Training (PR.AT)

PR.AT-01 **Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind**

- Information Security Policy
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Security Awareness and Training Policy
- Acceptable Use of Information Technology Resource Policy

PR.AT-02 **Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind**

- Information Security Policy
- Personnel Security Policy
- Physical and Environmental Protection Policy
- Security Awareness and Training Policy
- Access Control Policy
- Account Management/Access Control Standard
- Authentication Tokens Standard
- Configuration Management Policy
- Identification and Authentication Policy
- Acceptable Use of Information Technology Resource Policy

Protect: Data Security (PR.DS)

PR.DS-01 **The confidentiality, integrity, and availability of data-at-rest are protected**

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Encryption Standard
- Incident Response Policy
- Information Security Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Patch Management Standard

PR.DS-02 **The confidentiality, integrity, and availability of data-in-transit are protected**

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Encryption Standard
- Incident Response Policy
- Information Security Policy
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security
- Patch Management Standard

PR.DS-10 The confidentiality, integrity, and availability of data-in-use are protected

- Sanitization Secure Disposal Standard
- Secure Configuration Standard
- Secure System Development Life Cycle Standard
- Maintenance Policy
- Media Protection Policy
- Mobile Device Security

PR.DS-11 The confidentiality, integrity, and availability of data-in-use are protected

- Maintenance Policy
- Media Protection Policy

Protect: Platform Security (PR.PS)

PR.PS-01 Configuration management practices are established and applied

- Configuration Management Policy

PR.PS-02 Software is maintained, replaced, and removed commensurate with risk

- Maintenance Policy

PR.PS-03 Hardware is maintained, replaced, and removed commensurate with risk

- Sanitization Secure Disposal Standard
- Access Control Policy

PR.PS-04 Log records are generated and made available for continuous monitoring

- Identification and Authentication Policy

PR.PS-05 Installation and execution of unauthorized software are prevented

- Configuration Management Policy
- Secure Configuration Standard

PR.PS-06 Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle

- Sanitization Secure Disposal Standard

Protect: Technology Infrastructure Resilience (PR.IR)

PR.IR-01 **Networks and environments are protected from unauthorized logical access and usage**

- Remote Access Standard
- Mobile Device Security
- Encryption Standard
- Media Protection Policy
- System and Communications Protection Policy

PR.IR-02 **The organization's technology assets are protected from environmental threats**

- Secure Configuration Standard
- Secure System Development Life Cycle Standard
- Sanitization Secure Disposal Standard
- Maintenance Policy

PR.IR-03 **Mechanisms are implemented to achieve resilience requirements in normal and adverse situations**

- Secure System Development Life Cycle Standard
- System and Information Integrity Policy
- 802.11 Wireless Network Security Standard

PR.IR-04 **Adequate resource capacity to ensure availability is maintained**

- System and Information Integrity Policy

NIST FUNCTION:

Detect

Detect: Adverse Event Analysis (DE.AE)

DE.AE-02 Potentially adverse events are analyzed to better understand associated activities

- Auditing and Accountability Standard
- Secure Coding Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.AE-03 Information is correlated from multiple sources

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.AE-04 The estimated impact and scope of adverse events are understood

- Auditing and Accountability Standard
- System and Information Integrity Policy

DE.AE-06 Information on adverse events is provided to authorized staff and tools

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

DE.AE-07 Cyber threat intelligence and other contextual information are integrated into the analysis

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.AE-08 **Incidents are declared when adverse events meet the defined incident criteria**

- Computer Security Threat Response Policy
- Cyber Incident Response Standard
- Incident Response Policy
- Information Security Policy
- System and Information Integrity Policy
- Vulnerability Scanning Standard

Detect: Continuous Monitoring (DE.CM)

DE.CM-01 **Networks and network services are monitored to find potentially adverse events**

- Maintenance Policy
- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.CM-02 **The physical environment is monitored to find potentially adverse events**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.CM-03 **Personnel activity and technology usage are monitored to find potentially adverse events**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.CM-06 **External service provider activities and services are monitored to find potentially adverse events**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy
- Vulnerability Scanning Standard

DE.CM-09 **Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events**

- Auditing and Accountability Standard
- Security Logging Standard
- System and Information Integrity Policy

NIST FUNCTION:

Respond

Respond: Incident Management (RS.MA)

RS.MA-01 The incident response plan is executed in coordination with relevant third parties once an incident is declared

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

RS.MA-02 Incident reports are triaged and validated

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

RS.MA-03 Incidents are categorized and prioritized

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

RS.MA-04 Incidents are escalated or elevated as needed

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

RS.MA-05 The criteria for initiating incident recovery are applied

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

Respond: Incident Response Reporting and Communication (RS.CO)

RS.CO-02 Internal and external stakeholders are notified of incidents

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

RS.CO-03 Information is shared with designated internal and external stakeholders

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

RS.CO-3 Information is shared consistent with response plans.

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

Respond: Incident Analysis (RS.AN)

RS.AN-03 Analysis is performed to establish what has taken place during an incident and the root cause of the incident

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

RS.AN-06 Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved

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

RS.AN-07 Incident data and metadata are collected, and their integrity and provenance are preserved

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

RS.AN-08 An incident's magnitude is estimated and validated

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

Respond: Incident Mitigation (RS.MI)

RS.MI-01 Incidents are contained

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

RS.MI-02 Incidents are eradicated

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

NIST FUNCTION:

Recover

Recover: Incident Recovery Plan Execution (RC.RP)

RC.RP-01 The recovery portion of the incident response plan is executed once initiated from the incident response process

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

RC.RP-02 Recovery actions are selected, scoped, prioritized, and performed

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

RC.RP-03 The integrity of backups and other restoration assets is verified before using them for restoration

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

RC.RP-04 Critical mission functions and cybersecurity risk management are considered to establish post-incident operational norms

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

RC.RP-05 The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed

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

RC.RP-06 The end of incident recovery is declared based on criteria, and incident-related documentation is completed

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

Recover: Incident Recovery Communication (RC.CO)

RC.CO-03 Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders

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

RC.CO-04 Public updates on incident recovery are shared using approved methods and messaging

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

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
CenterforIntSec
@CISecurity
TheCISecurity
cisecurity