

OMB Control Number: 1670-NEW
OMB Expiration Date: MM/DD/YYYY



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



NCSR RESPONSE SCALE & QUESTION SET



Paperwork Reduction Act

The public reporting burden to complete this information collection is estimated at 2 hours per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and the completing and reviewing the collected information. The collection of information is voluntary. An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a currently valid OMB control number and expiration date. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to DHS/NPPD/CS&C, 245 Murray Lane, SW, Mail Stop 0612, Arlington, VA 20598-0640 or SLTTCyber@HQ.DHS.GOV ATTN: PRA [OMB Control No. 1670-NEW].

| Score | Maturity Level <i>The recommended minimum maturity level is set at a score of 5 and higher</i> |
|-------|---|
| 7 | Optimized: Your organization has formally documented policies, standards, and procedures. Implementation is tested, verified, and reviewed regularly to ensure continued effectiveness. |
| 6 | Tested and Verified: Your organization has formally documented policies, standards, and procedures. Implementation is tested and verified. |
| 5 | Implementation in Process: Your organization has formally documented policies, standards, and procedures and are in the process of implementation. |
| 5 | Risk Formally Accepted: Your organization has chosen not to implement based on a risk assessment. |
| 4 | Partially Documented Standards and/or Procedures: Your organization has a formal policy in place and begun the process of developing documented standards and/or procedures to support the policy. |
| 3 | Documented Policy: Your organization has a formal policy in place. |
| 2 | Informally Performed: Activities and processes may be substantially performed and technologies may be available to achieve this objective, but they are undocumented and/or not formally approved by management. |
| 1 | Not Performed: Activities, processes and technologies are not in place to achieve the referenced objective. |

Demographics

(CSF) Demographics

| | |
|---|--|
| (NCSR)Demo 1: Executive Reporting: | Do your top-level decision-makers receive periodic (at least annual) reports on the status of information risks, controls, and/or security from the departments, divisions, and/or agencies within your organization? |
| (NCSR)Demo 2: Cyber Security Executive Mandates: | Has your organization adopted or established a set of cybersecurity executive mandates, laws, statutes, approved legislation, policies, or standards to help guide the implementation of information security controls across your organization? |
| (NCSR)Demo 3: Security Framework: | Which control frameworks and/or security methodologies are your organization's information security controls based on? Select all that apply. |
| (NCSR)Demo 4: FTE Size: | How many full-time equivalent (FTEs) employees/contractors are there in your organization? |
| (NCSR)Demo 5: IT FTE: | How many full-time equivalent employees are there in your IT? |
| (NCSR)Demo 6: Security FTE: | How many full-time equivalent employees have security related duties? |
| (NCSR)Demo 7: IT Outsourcing: | What part of your IT operation is outsourced? |
| (NCSR)Demo 8: Security Outsourcing: | What part of your security operation is outsourced? |

Identify

(CSF) Identify.Asset Management

| | |
|-----------------|---|
| ID.AM-1: | Physical devices and systems within the organization are inventoried. |
| ID.AM-2: | Software platforms and applications within the organization are inventoried |
| ID.AM-3: | Organizational communication and data flows are mapped |
| ID.AM-4: | External information systems are catalogued |
| ID.AM-5: | Resources (e.g., hardware, devices, data, time, and software) are prioritized based on their classification, criticality, and business value |
| ID.AM-6: | Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established |



(CSF) Identify.Business Environment

| | |
|-----------------|--|
| ID.BE-1: | The organization's role in the supply chain is identified and communicated |
| ID.BE-2: | The organization's place in critical infrastructure and its industry sector is identified and communicated |
| ID.BE-3: | Priorities for organizational mission, objectives, and activities are established and communicated |
| ID.BE-4: | Dependencies and critical functions for delivery of critical services are established |
| ID.BE-5: | Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) |

(CSF) Identify.Governance

| | |
|-----------------|--|
| ID.GV-1: | Organizational information security policy is established. |
| ID.GV-2: | Information security roles & responsibilities are coordinated and aligned with internal roles and external partners |
| ID.GV-3: | Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed |
| ID.GV-4: | Governance and risk management processes address cybersecurity risks |

(CSF) Identify.Risk Assessment

| | |
|-----------------|---|
| ID.RA-1: | Asset vulnerabilities are identified and documented |
| ID.RA-2: | Cyber threat intelligence and vulnerability information is received from information sharing forums and sources |
| ID.RA-3: | Threats, both internal and external, are identified and documented |
| ID.RA-4: | Potential business impacts and likelihoods are identified |
| ID.RA-5: | Threats, vulnerabilities, likelihoods, and impacts are used to determine risk |
| ID.RA-6: | Risk responses are identified and prioritized |



(CSF) Identify.Risk Management Strategy

| | |
|-----------------|---|
| ID.RM-1: | Risk management processes are established, managed, and agreed to by organizational stakeholders |
| ID.RM-2: | Organizational risk tolerance is determined and clearly expressed |
| ID.RM-3: | The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis |

Protect

(CSF) Protect.Access Control

| | |
|-----------------|---|
| PR.AC-1: | Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes |
| PR.AC-2: | Physical access to assets is managed and protected |
| PR.AC-3: | Remote access is managed |
| PR.AC-4: | Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties |
| PR.AC-5: | Network integrity is protected, incorporating network segregation where appropriate |

(CSF) Protect.Awareness and Training

| | |
|-----------------|---|
| PR.AT-1: | All users are informed and trained |
| PR.AT-2: | Privileged users understand roles & responsibilities |
| PR.AT-3: | Third-party stakeholders (e.g., suppliers, customers, partners) understand roles & responsibilities |
| PR.AT-4: | Senior executives understand roles & responsibilities |
| PR.AT-5: | Physical and information security personnel understand roles & responsibilities |

(CSF) Protect.Data Security

| | |
|-----------------|--|
| PR.DS-1: | Data-at-rest is protected |
| PR.DS-2: | Data-in-transit is protected |
| PR.DS-3: | Assets are formally managed throughout removal, transfers, and disposition |
| PR.DS-4: | Adequate capacity to ensure availability is maintained |
| PR.DS-5: | Protections against data leaks are implemented |
| PR.DS-6: | Integrity checking mechanisms are used to verify software, firmware, and information integrity |
| PR.DS-7: | The development and testing environment(s) are separate from the production environment |

(CSF) Protect.Information Protection Process and Procedures

| | |
|------------------|--|
| PR.IP-1: | A baseline configuration of information technology/industrial control systems is created and maintained |
| PR.IP-2: | A System Development Life Cycle to manage systems is implemented |
| PR.IP-3: | Configuration change control processes are in place |
| PR.IP-4: | Backups of information are conducted, maintained, and tested periodically |
| PR.IP-5: | Policy and regulations regarding the physical operating environment for organizational assets are met |
| PR.IP-6: | Data is destroyed according to policy |
| PR.IP-7: | Protection processes are continuously improved |
| PR.IP-8: | Effectiveness of protection technologies is shared with appropriate parties |
| PR.IP-9: | Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed |
| PR.IP-10: | Response and recovery plans are tested |
| PR.IP-11: | Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) |
| PR.IP-12: | A vulnerability management plan is developed and implemented |



(CSF) Protect.Maintenance

| | |
|-----------------|--|
| PR.MA-1: | Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools |
| PR.MA-2: | Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access |

(CSF) Protect.Protective Technology

| | |
|-----------------|--|
| PR.PT-1: | Audit/log records are determined, documented, implemented, and reviewed in accordance with policy |
| PR.PT-2: | Removable media is protected and its use restricted according to policy |
| PR.PT-3: | The principle of least functionality is incorporated by configuring systems to provide only essential capabilities |
| PR.PT-4: | Communications and control networks are protected |



Detect

(CSF) Detect.Anomalies and Events

| | |
|-----------------|---|
| DE.AE-1: | A baseline of network operations and expected data flows for users and systems is established and managed |
| DE.AE-2: | Detected events are analyzed to understand attack targets and methods |
| DE.AE-3: | Event data are aggregated and correlated from multiple sources and sensors |
| DE.AE-4: | Impact of events is determined |
| DE.AE-5: | Incident alert thresholds are established |

(CSF) Detect.Security Continuous Monitoring

| | |
|-----------------|--|
| DE.CM-1: | The network is monitored to detect potential cybersecurity events |
| DE.CM-2: | The physical environment is monitored to detect potential cybersecurity events |
| DE.CM-3: | Personnel activity is monitored to detect potential cybersecurity events |
| DE.CM-4: | Malicious code is detected |
| DE.CM-5: | Unauthorized mobile code is detected |
| DE.CM-6: | External service provider activity is monitored to detect potential cybersecurity events |
| DE.CM-7: | Monitoring for unauthorized personnel, connections, devices, and software is performed |
| DE.CM-8: | Vulnerability scans are performed |

(CSF) Detect.Detection Process

| | |
|---------------|---|
| DE.DP: | Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events. |
|---------------|---|

Respond

(CSF) Respond.Response Planning

RS.RP-1: Response plan is executed during or after an event

(CSF) Respond.Communications

RS.CO-1: Personnel know their roles and order of operations when a response is needed

RS.CO-2: Events are reported consistent with established criteria

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

RS.CO-4: Coordination with stakeholders occurs consistent with response plans

RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness

(CSF) Respond.Analysis

RS.AN-1: Notifications from detection systems are investigated

RS.AN-2: The impact of the incident is understood

RS.AN-3: Forensics are performed

RS.AN-4: Incidents are categorized consistent with response plans

(CSF) Respond.Mitigation

RS.MI-1: Incidents are contained

RS.MI-2: Incidents are mitigated

RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

(CSF) Respond.Improvements

RS.IM-1: Response plans incorporate lessons learned

RS.IM-2: Response strategies are updated

Recover

(CSF) Recover.Recovery Planning

RC.RP-1: Recovery plan is executed during or after an event

(CSF) Recover.Improvements

RC.IM-1: Recovery plans incorporate lessons learned

RC.IM-2: Recovery strategies are updated

(CSF) Recover.Communications

RC.CO-1: Public relations are managed

RC.CO-2: Reputation after an event is repaired

RC.CO-3: Recovery activities are communicated to internal stakeholders and executive and management teams

Privacy

Privacy

PC - 1: Does your organization have a privacy officer?

PC - 2: Does your organization have clearly defined processes to report a breach of PII/PHI?

Post Survey Questions

General

(Post Survey) Question 1: What are your top 5 security concerns?

(Post Survey) Question 2: Were you able to answer all of the assessment questions?

(Post Survey) Question 3: How long did it take you to complete this assessment (including time spent researching answers off-line)