# **NEW MEXICO CYBERSECURITY OFFICE**

# **Cybersecurity Risk Assessment Survey FY2025**

**

## **Organization Information**

This assessment aligns with the NIST CSF 2.0 framework, ensuring a consistent and comprehensive evaluation of cybersecurity practices for state agencies, departments, and offices. This enables state entities to meet the requirements set forth in the executive order and enhance their overall security posture.

Please provide the following information regarding your organization:

|  |  |
| --- | --- |
| Entity Name (i.e., Agency, Department, etc.) \*: | Click or tap here to enter text. |
| Agency Leader Name \*: | Click or tap here to enter text. |
| Agency Leader Email \*: | Click or tap here to enter text. |
| Agency Chief Information Officer (CIO) or IT Lead Name \*: | Click or tap here to enter text. |
| Agency Chief Information Officer (CIO) or IT Lead Email \*: | Click or tap here to enter text. |
| Designated IT/Cybersecurity Point of Contact (POC) Name \*: | Click or tap here to enter text. |
| Provide POC E-mail Address \*: | Click or tap here to enter text. |

**Assessment Maturity Scores**

Each domain group will contain questions scored on a 0-5 scale, with **0** indicating **"Not Implemented"** and **5** indicating **"Optimized".** Additionally, there will be one or more open-ended questions. The open-ended questions allow the entity to describe the implementation and capabilities referenced in the scored questions in their own words.

|  |  |
| --- | --- |
| **Maturity Level** | **Level Description** |
| **Level 0: Not implemented** | The entity has not implemented the control and is not taking any actions to develop or implement the control. |
| **Level 1: Initial**  | The entity has some awareness and is taking first steps, but practices are inconsistent and not formalized. |
| **Level 2: Emerging** | The entity has recognized the need for structured practices and is developing processes that are not yet fully established or consistent. |
| **Level 3: Established** | The entity has implemented structured practices consistently applied, with a clear process for regular review and improvement. |
| **Level 4: Advanced** | The entity has a well-managed and measured approach, with practices that are integrated into overall operations and contribute to strategic goals. |
| **Level 5: Optimized** | The entity demonstrates best-in-class practices, continuously innovates, and may set benchmarks for others in the control group's domain. |

**GOVERN**

The Govern domain in NIST CSF 2.0 is crucial for integrating cybersecurity into the broader organizational governance framework, thereby enhancing risk management, compliance, accountability, and resource allocation. This holistic approach helps build a resilient organization capable of addressing evolving cyber threats.

### **Organizational Context**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity uses a periodic process to identify internal and external stakeholders that can impact its cybersecurity posture and potential impacts are known and understood.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity regularly communicates its cybersecurity expectations to both internal and external stakeholders, ensuring that the relevant roles and responsibilities regarding cybersecurity are clearly conveyed to each group.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity periodically communicates its policies, procedures, and expectations regarding the protection of private data to internal and external stakeholders, as applicable.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity uses a periodic process to identify and classify cybersecurity dependencies based on their criticality to the entity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Stakeholder (internal and external) dependencies are understood and classified accordingly.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity uses a periodic process to identify and understand cybersecurity compliance obligations, including legal and regulatory requirements related to privacy and civil liberties.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity adopts cybersecurity policies, procedures, and processes to ensure compliance with legal and regulatory obligations.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain below:** |
| Click or tap here to enter text. |

| **Organizational Context – Open Ended Questions** |
| --- |
| 1. How does the entity ensure that its cybersecurity framework aligns with and supports its core mission, legal obligations, and operational objectives? \*

Response Guidelines:* The entity's mission helps identify cybersecurity risks that could hinder its goals.
* The legal, regulatory, and contractual requirements for cybersecurity are understood and handled effectively.
* The key objectives, capabilities, and services that the entity relies on are understood and communicated.
 |
| Click or tap here to enter text. |
| 1. How does the entity communicate and align its cybersecurity risk management practices with the expectations and requirements of its stakeholders? \*

Response Guidelines:* Cybersecurity risk management needs and expectations for both internal and external stakeholders are communicated through established channels.
* The key objectives, capabilities, and services that external stakeholders expect and rely on are understood and communicated.
 |
| Click or tap here to enter text. |

**Risk Management Strategy**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity periodically communicates its acceptable levels of cybersecurity risk to internal and external stakeholders, ensuring a shared understanding across the entity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity uses a standardized process to calculate, document, categorize, and prioritize cybersecurity risks based on their criticality to the entity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity adopts cybersecurity risk management processes that are established, managed, and agreed upon by internal and external stakeholders relevant to their roles.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. The entity integrates its cybersecurity risk management processes into its overall risk management strategy and periodically reviews these processes for effectiveness, making necessary adjustments to ensure continuous improvement.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain below:** |
| Click or tap here to enter text. |

| **Risk Management Strategy – Open Ended Questions** |
| --- |
| 1. How does the entity establish, communicate, and align its risk management objectives and strategies to effectively manage cybersecurity risks? \*

Response Guidelines:* Entity stakeholders have established and agreed on risk management objectives.
* The entity’s willingness to take risk and acceptable levels of risk are communicated through defined channels.
* The strategic direction that describes appropriate risk response options and characterizes strategic opportunities (i.e., positive risks) are established, communicated, and included in cybersecurity risk discussions.
* Established communication lines exist within the entity for discussing cybersecurity risks, including those from suppliers and other third parties.
 |
| Click or tap here to enter text. |
| 1. How are cybersecurity risk management activities standardized and integrated within the broader enterprise risk management framework? \*

Response Guidelines:* Cybersecurity risk management activities and outcomes are integrated into the enterprise risk management processes.
* A standardized method is used to calculate, document, categorize, and prioritize cybersecurity risks, and this method is communicated effectively.
 |
| Click or tap here to enter text. |

### **Roles, Responsibilities, and Authorities**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity's leadership agrees on their roles and responsibilities in supporting, sponsoring, and assessing the entity's cybersecurity strategy.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity defines cybersecurity roles and responsibilities for the workforce and entity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity allocates adequate resources commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures that all personnel, including third-party stakeholders, are aware of their cybersecurity roles and responsibilities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity integrates cybersecurity into human resources practices (e.g., personnel screening, onboarding, offboarding).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain below:** |
| Click or tap here to enter text. |

| **Roles, Responsibilities, and Authorities – Open Ended Questions** |
| --- |
| 1. How does the entity integrate and manage cybersecurity within its leadership, human resources, and overall risk management practices? \*

Response Guidelines:* Leadership promotes a risk-aware, ethical, and continually improving culture.
* Roles, responsibilities, and authorities for managing cybersecurity risks are established, communicated, and enforced.
* Cybersecurity is integrated into human resources practices.
 |
| Click or tap here to enter text. |

### **Policies, Procedures, and Processes**\*

|  |  **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. The entity establishes, communicates, and enforces cybersecurity policies, procedures, and processes, and regularly reviews and updates them to ensure they remain effective and current.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain below:** |
| Click or tap here to enter text. |

| **Policies, Procedures, and Processes – Open Ended Questions** |
| --- |
| 1. How are cybersecurity risk policies established and managed? \*

Response Guidelines:* Cybersecurity risk policies are established through a defined process involving relevant stakeholders and subject matter experts.
* There is a process to effectively communicate and enforce cybersecurity risk policies to designated personnel.
* There is a process to review and update cybersecurity risk policies annually.
 |
| Click or tap here to enter text. |

### **Supply Chain Risk Management**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity communicates cybersecurity roles and responsibilities to third-party stakeholders (e.g., suppliers, customers, partners).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity understands supply chain risks before entering agreements or contracts with potential third-party stakeholders (e.g., suppliers, customers, partners).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity inventories and prioritizes suppliers based on their criticality.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity outlines cybersecurity responsibilities for third-party stakeholders in agreements or contracts.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity understands and integrates supply chain risks into the enterprise risk management strategy, incident planning, response, and recovery activities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain below:** |
| Click or tap here to enter text. |

| **Supply Chain Risk Management – Open Ended Questions** |
| --- |
| 1. How does the entity establish, assess, and refine its cybersecurity supply chain risk management processes to ensure robust protection against potential threats? \*

Response Guidelines:* There is a process to establish and verify cybersecurity supply chain risk management, with clearly defined roles and responsibilities involved.
* There is a process to develop risk management requirements for the supply chain.
* Supply chain risk assessments are conducted to reduce risk when contracting suppliers.
 |
| Click or tap here to enter text. |
| 1. How does the organization integrate supply chain risk management into its contractual agreements, supplier management processes, and broader cybersecurity strategies? \*

Response Guidelines:* Supply chain risk management requirements are integrated into contracts.
* Suppliers are inventoried and prioritized.
* Cybersecurity supply chain risk management is integrated into other cybersecurity processes.
 |
| Click or tap here to enter text. |

**Governance and Oversight**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity clearly defines and communicates cybersecurity risk management roles, responsibilities across the entity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity's leadership and governance structures actively support cybersecurity risk management.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity conducts regular reviews and updates of its cybersecurity governance framework to ensure its continued effectiveness.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity has a documented process for escalating cybersecurity risks to senior management and agency leadership
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures that all employees are aware of and understand their roles and responsibilities related to cybersecurity governance.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity has established metrics and Key Performance Indicators (KPIs) to measure the effectiveness of its cybersecurity governance framework.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain below:** |
| Click or tap here to enter text. |

| **Governance and Oversight – Open Ended Questions** |
| --- |
| 1. How are cybersecurity risk management strategies managed, updated, and reviewed? \*

Response Guidelines:* Cybersecurity risk policies are established through a defined process involving relevant stakeholders and subject matter experts.
* There is a process to effectively communicate and enforce cybersecurity risk policies to designated personnel.
* There is a process to update cybersecurity risk policies.
 |
| Click or tap here to enter text. |

## **IDENTIFY**

The Identify domain in NIST CSF 2.0 is crucial for establishing a solid foundation for managing cybersecurity risks. By identifying and understanding assets, business environments, governance structures, risks, and supply chain dependencies, organizations can prioritize their cybersecurity efforts and allocate resources effectively to protect against potential threats. This domain sets the stage for the subsequent functions of Protect, Detect, Respond, and Recover.

### **Asset Management**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity maintains an inventory of all physical devices and systems.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity maintains an inventory of all software platforms and applications.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity maintains a centralized repository of information about data, such as meaning, relationships to other data, origin, usage, and format.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity's communication and data flows are mapped and updated regularly
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Communication and data flow maps include both internal and external network connections.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. The entity inventories and classifies its assets based on their criticality and conducts periodic audits to verify the accuracy and completeness of the inventory.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Asset Management – Open Ended Questions** |
| --- |
| 1. How are assets (systems, hardware, software, services, and data) inventoried and managed within the entity? \*

Response Guidelines:* There is a process to maintain inventories of hardware, software, services, systems, and external services.
* Assets are prioritized by classification and criticality.
* Assets are managed throughout each phase of the life cycle.
 |
| Click or tap here to enter text. |

### **Risk Assessment**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity conducts regular risk assessments to identify potential cybersecurity threats and vulnerabilities.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. Entity uses a standardized methodology to evaluate and prioritize risks based on their potential impact and likelihood.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. Entity documents and communicates risk assessment results to relevant stakeholders within the organization.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. Entity updates its risk assessments whenever there are significant changes to its operating environment or threat landscape.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. Entity integrates risk assessment findings into its overall risk management strategy and decision-making processes.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. Entity uses both automated tools and human oversight for conducting risk assessments.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. Risk assessments include an evaluation of the effectiveness of existing security controls and measures.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1. The organization involves senior management in the risk assessment process.
 | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Risk Assessment – Open Ended Questions** |
| --- |
| 1. What is the entity's process for identifying, prioritizing, and understanding various threats and vulnerabilities, including how it handles internal and external threats, the prioritization of vulnerabilities, and the response to vulnerability disclosures? \*

Response Guidelines:* There is an identification and prioritization process for vulnerabilities, internal and external threats, and potential impacts and exploitation of vulnerabilities.
* Potential or realized internal and external threats to the entity are identified and recorded.
* There is a process for receiving, analyzing, and responding to vulnerability disclosures established.
 |
| Click or tap here to enter text. |
| 1. What is the entity’s process for formulating risk responses, and handling changes to the risk profile? \*

Response Guidelines:* Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risks and inform risk response prioritization.
* Risk responses are chosen, prioritized, planned, tracked, and communicated.
* Changes and exceptions to risk are managed, assessed, recorded, and tracked.
 |
| Click or tap here to enter text. |
| 1. What are the integrity and security considerations related to suppliers and external hardware/software utilized by the entity? \*

Response Guidelines:* The integrity of acquired and used hardware and software is validated.
* Critical suppliers are assessed prior to onboarding, with assessments based on business and cybersecurity requirements.
 |
| Click or tap here to enter text. |

### **Improvement**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity identifies improvements from security tests and exercises, including those conducted in coordination with suppliers and relevant third parties.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity establishes, communicates, maintains, and improves incident response plans and other cybersecurity plans.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity regularly reviews and updates cybersecurity policies and procedures.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Improvement – Open Ended Questions** |
| --- |
| 1. How is the entity continually improving cybersecurity policies, processes, and procedures? \*

Response Guidelines:* Self-assessments are performed on critical services.
* Independent audits of the entity are performed, and the frequency is specified.
* Cybersecurity policies, processes, and procedures are reviewed frequently to incorporate lessons learned.
* Incident response and cybersecurity plans that impact operations are communicated and reviewed for enhancements regularly.
 |
| Click or tap here to enter text. |

## **PROTECT**

The Protect domain in NIST CSF 2.0 is essential for implementing safeguards that ensure the security and resilience of critical infrastructure services. By focusing on identity management, awareness and training, data security, information protection processes, maintenance, and protective technologies, organizations can limit the impact of potential cybersecurity events and maintain the integrity and availability of their systems and data. This domain supports the overall goal of reducing cybersecurity risks and enhancing organizational resilience.

### **Identity Management, Authentication, and Access Control**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity issues, manages, verifies, revokes, and audits identities and credentials for authorized devices, users, and processes.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity properly identifies, manages, and protects private and sensitive data.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity has policies and procedures in place that protect physical access to assets.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity requires the use of multi-factor authentication (MFA) for remote access to systems.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity manages access permissions and authorizations, incorporating the principles of least privilege and separation of duties.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity protects network integrity by implementing network security practices such as Intrusion Detection and Prevention Systems (IDS/IPS), network monitoring, traffic logging, and network segmentation.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Identity Management, Authentication, and Access Control – Open Ended Questions** |
| --- |
| 1. How does the entity enforce identity management, authentication, and access control requirements and safety precautions? \*

Response Guidelines:* The entity manages authorization and authentication for assets (users, services, and hardware).
* Processes are in place for verifying and assigning credentials based on individual responsibilities.
* Access policies (permissions, entitlements, authorizations) are managed, enforced, and reviewed, incorporating the principles of least privilege and separation of duties.
* Access to physical assets is managed, monitored, and enforced based on risk levels.
 |
| Click or tap here to enter text. |

### **Awareness and Training**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity ensures privileged users understand their roles and responsibilities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures senior executives understand their roles and responsibilities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity provides role-based cybersecurity training and awareness to specialized roles.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity provides role-based cybersecurity training and awareness to contractors, suppliers, and other third parties.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures personnel and contractors understand their roles and responsibilities regarding the collection and management of protected and private data.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Awareness and Training – Open Ended Questions** |
| --- |
| 1. How frequently is general and role-based cybersecurity training provided to personnel? \*

Response Guidelines:* General cybersecurity training is provided to all personnel, including employees, contractors, partners, and suppliers, on a specified frequency.
* Specialized roles receive role-based training to enhance their skills and knowledge on a regular basis.
 |
| Click or tap here to enter text. |

### **Data Security**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity protects data at both stages:.
* Data at Rest - Stored data not actively moving or being accessed.
* Data in Transit - Data actively moving between locations
 | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  | [ ]  |
| 1. Entity implements protections against data leaks (e.g. Role based access control, data masking, intrusion detection/prevention systems, and secure coding practices).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity uses methods to verify data integrity on software, firmware, and information.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures that development and testing environments are separate from the production environment.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Data Security – Open Ended Questions** |
| --- |
| 1. How does the entity protect the confidentiality, integrity, and availability of data? \*

Response Guidelines:* Sensitive data is protected at rest, and in transit.
* Sensitive data is protected from unauthorized use and disclosure.
* Data backups are created frequently and maintained properly.
 |
| Click or tap here to enter text. |

### **Platform Security**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity ensures a baseline configuration of information technology/industrial control systems is created and maintained.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures the principle of least functionality is incorporated by configuring systems to provide only essential capabilities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures protective measures are in place to verify the installation of new software and prevent installation and access of unauthorized and prohibited software.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity ensures policy and regulations regarding the physical operating environment for organizational assets are met.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Platform Security – Open Ended Questions** |
| --- |
| 1. How does the entity ensure security and functionality through system configuration and software management? \*

Response Guidelines:* Default settings are established and applied to ensure that systems operate with only the necessary functionalities.
* Measures are in place to ensure the correct installation of new software and to prevent the installation and access of unauthorized software.
 |
| Click or tap here to enter text. |
| 1. What is the process to maintain hardware and software, monitor system activities, and protect software? \*

Response Guidelines:* There is a process for maintaining, replacing, and removing software and hardware commensurate with risk.
* The entity promotes continuous monitoring to generate and share log records.
* Entity-developed software is protected during the software development life cycle.
 |
| Click or tap here to enter text. |

### **Technology Infrastructure Resilience**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity implements network protection measures to prevent unauthorized access and usage.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity protects physical assets from environmental threats (e.g., flooding, fire, wind, excessive heat, and humidity).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity implements mechanisms (e.g., failsafe, load balancing, hot swap) to achieve resilience requirements in normal and adverse situations.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Technology Infrastructure Resilience – Open Ended Questions** |
| --- |
| 1. How does the entity ensure the security, reliability, and scalability of its physical and digital infrastructure? \*

Response Guidelines:* Strategies and technologies are used to prevent unauthorized access to and usage of the network.
* Physical assets are safeguarded against environmental risks such as flooding, fire, wind, and extreme temperatures.
* Requirements and mechanisms are in place to ensure the reliability of systems and infrastructure under both normal and adverse conditions.
* The entity monitors resource usage, forecasts future needs, and scales resources accordingly.
 |
| Click or tap here to enter text. |

## **DETECT**

The Detect domain in NIST CSF 2.0 is critical for identifying cybersecurity events in a timely manner. By focusing on detecting anomalies and events, implementing continuous monitoring, and maintaining robust detection processes, organizations can quickly identify and respond to potential threats. This domain supports the overall goal of minimizing the impact of cybersecurity incidents and enhancing the organization's ability to maintain the integrity, confidentiality, and availability of its systems and data.

### **Continuous Monitoring**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity monitors the network to detect potential risks to cybersecurity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity monitors the physical environment to detect potential risks to cybersecurity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity monitors personnel activity to detect potential risks to cybersecurity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity monitors external service provider activity to detect potential risks to cybersecurity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity monitors computing hardware, software, and runtime environments for potential risks to cybersecurity.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Continuous Monitoring – Open Ended Questions** |
| --- |
| 1. What mechanisms are in place to continuously monitor the environment and assets for adverse events? \*

Response Guidelines:* Assets, computing software, software, and runtime environments are monitored to identify anomalies or indicators of compromise.
* User activity and the physical environment are monitored to identify potential incidents.
* Mechanisms are in place to monitor external service providers to identify potential adverse events.
 |
| Click or tap here to enter text. |

### **Adverse Event Analysis**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity establishes and manages a baseline of network operations and expected data flows for users and systems.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity analyzes detected events to understand attack targets and methods.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity collects and correlates event data from multiple sources and sensors.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity communicates event detection information to appropriate parties (internal and external).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Adverse Event Analysis – Open Ended Questions** |
| --- |
| 1. How are potential cyber threats and ongoing cyber incidents analyzed to prevent future attacks? \*

Response Guidelines:* There is a process to analyze potential threats and cyber incidents that have occurred.
* Specific sources are gathered during cyber incident analysis.
* Criteria is established to declare that a cyber incident has occurred.
 |
| Click or tap here to enter text. |
| 1. How are cyber threat information and contextual information shared? \*

Response Guidelines:* Cyber incident data is shared with designated personnel and tools through established processes.
* Policies and standards are in place to guarantee that relevant cyber incident data and other contextual information are included in the analysis.
 |
| Click or tap here to enter text. |

## **RESPOND**

The Respond domain in NIST CSF 2.0 is essential for managing the impact of cybersecurity incidents effectively. By focusing on response planning, communication, analysis, mitigation, and continuous improvement, organizations can ensure a coordinated and effective response to incidents. This domain supports the overall goal of minimizing the impact of cybersecurity events and enhancing the organization’s resilience against future threats.

### **Incident Management**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity executes the incident response plan in coordination with relevant third parties once an incident is declared.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity regularly tests and updates incident response plans according to a defined schedule.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity triages and validates incident reports to confirm they necessitate incident response activities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity categorizes and prioritizes incidents according to documented procedures.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity escalates incidents as needed to designated stakeholders (internal and external).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity defines criteria for initiating incident recovery.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Incident Management – Open Ended Questions** |
| --- |
| 1. How is an incident declared and managed? \*

Response Guidelines:* Third parties are included in the incident response activities through defined processes.
* There is a process to review, analyze, categorize, prioritize, and escalate (as needed) incidents.
* Criteria are established for starting incident recovery activities and processes.
 |
| Click or tap here to enter text. |

### **Incident Analysis**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity performs incident analysis to understand incident events and the root cause of the incident.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity records and maintains incident analysis and investigation activities, including data and metadata.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity analyzes the outcome of incidents for indicators of compromise and evidence of persistence.
 |[ ] [ ]  [ ]  |[ ] [ ]  [ ]  | [ ]  |
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Incident Analysis – Open Ended Questions** |
| --- |
| 1. How is incident analysis performed? \*

Response Guidelines:* A specific process is used to determine what has taken place during an incident and to identify the root cause.
* Specific actions are performed during an incident investigation, and record integrity is preserved through defined methods.
* The entity has a method to estimate and validate an incident's magnitude.
 |
| Click or tap here to enter text. |

### **Incident Response Reporting and Communication**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity notifies and updates stakeholders (internal and external) through secure methods during incident response activities.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Incident Response Reporting and Communication – Open Ended Questions** |
| --- |
| 1. How are stakeholders notified during incidents? \*

Response Guidelines:* Incident details are communicated and stakeholders, both internal and external.
 |
| Click or tap here to enter text. |

### **Incident Mitigation**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity establishes and maintains infrastructure to automatically contain and eradicate cyber incidents.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity enables incident responders to manually select and perform additional containment and eradication actions.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity outlines procedures for containment and eradication actions for third-party cybersecurity services and vendors.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Incident Mitigation – Open Ended Questions** |
| --- |
| 1. What is the process for mitigating incidents? \*

Response Guidelines:* Containment actions are performed in the event of an incident.
* Eradication actions are performed in the event of an incident.
 |
| Click or tap here to enter text. |

## **RECOVER**

The Recover domain in NIST CSF 2.0 is crucial for ensuring that organizations can quickly and effectively restore systems and services affected by cybersecurity incidents. By focusing on recovery planning, continuous improvement, and effective communication, organizations can minimize the impact of incidents on business operations and enhance their overall resilience. This domain supports the overall goal of maintaining the integrity, confidentiality, and availability of organizational systems and data, even in the face of cybersecurity challenges.

### **Incident Recovery Plan Execution**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity defines starting criteria for the recovery portion of the incident response plan during the incident response process.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity tests and updates incident recovery plans on a documented and specified frequency.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity determines and prioritizes recovery activities based on the entity’s understanding of risk and needs.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity regularly tests system backups to confirm they are recoverable in the event of a cybersecurity incident.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity includes critical functions and cybersecurity risk management within restoration activities and restores them in order of priority.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity verifies restored assets for correctness and adequacy before putting them back online.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity defines criteria to declare the end of incident recovery activities, including completing any incident-related documents.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Incident Recovery Plan Execution – Open Ended Questions** |
| --- |
| 1. How are recovery activities executed within the Incident Response Plan/Playbook? \*

Response Guidelines:* The criteria to initiate and end recovery activities are defined.
* The verification process ensures that assets, systems, and services are operational before ending recovery actions.
* Incident-related documentation must be completed before ending recovery actions.
* Specific individuals or roles are responsible for collecting and reviewing incident-related documentation.
 |
| Click or tap here to enter text. |

### **Incident Recovery Communication**\*

|  | **0** | **1** | **2** | **3** | **4** | **5** | **N/A** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1. Entity communicates incident recovery activities and restoration progress to designated stakeholders (internal and external).
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| 1. Entity shares updates on incident recovery using approved methods and messaging.
 |[ ] [ ] [ ] [ ] [ ] [ ] [ ]
| **If you selected “N/A” to any of the questions above, please explain why:** |
| Click or tap here to enter text. |

| **Incident Recovery Communication – Open Ended Questions** |
| --- |
| 1. What are the organizations common communication practices within regarding incident recovery activities? \*

Response Guidelines:* Strategies and processes are in place to share recovery information and communicate progress during recovery activities.
* Roles and responsibilities are assigned to members involved in the recovery process.
* A specific method is used to communicate incident recovery updates with the public.
 |
| Click or tap here to enter text. |

## **NIST Privacy Framework**

### **Govern**

The Govern domain in the NIST Privacy Framework is crucial for establishing and maintaining a governance structure that supports privacy risk management. This domain ensures that privacy policies, procedures, and roles are clearly defined and aligned with organizational objectives. Effective governance enhances accountability, compliance, and resource allocation, thereby fostering a culture of privacy within the organization and ensuring that privacy risks are managed proactively.

| **NIST Privacy Framework – Open Ended Questions** |
| --- |
| 1. What governance structures and policies does the organization have in place to manage privacy risks, particularly those related to PII and sensitive data, and how are they communicated across the organization? \*

Response Guidelines:* Establish a dedicated Data Privacy Office or Privacy Governance Committee responsible for overseeing privacy risk management.
* Implement comprehensive privacy policies and procedures that outline the handling, protection, and management of PII and sensitive data.
* Conduct regular privacy training programs to ensure all employees understand and comply with privacy policies and procedures.
* Use multiple communication channels, such as intranet, emails, and workshops, to disseminate privacy policies and updates across the organization.
 |
| Click or tap here to enter text. |
| 1. How does your organization ensure accountability and oversight for privacy risk management, specifically in the context of PII and sensitive data? \*

Response Guidelines:* Assign clear roles and responsibilities for privacy risk management to specific individuals or teams, such as a Chief Privacy Officer or Data Protection Officer.
* Implement regular audits and assessments to ensure compliance with privacy policies and identify areas for improvement.
* Utilize a robust incident management process to track and respond to privacy breaches, ensuring accountability at all levels.
* Examples of data involved include personal identifiers (e.g., names, social security numbers), financial information (e.g., credit card details), health records, and biometric data.
 |
| Click or tap here to enter text. |

### **Identify**

The Identify domain in the NIST Privacy Framework is essential for developing an understanding of privacy risks to systems, assets, data, and capabilities. This foundational step enables organizations to manage privacy risks effectively and ensure that privacy considerations are integrated into the organizational risk management process. By identifying and understanding privacy risks, organizations can better protect individual privacy and build trust with stakeholders.

| **NIST Privacy Framework – Open Ended Questions** |
| --- |
| 1. Can you describe the process your organization uses to identify and document privacy risks associated with your data processing activities, particularly concerning PII and sensitive data? \*

Response Guidelines:* Conduct a comprehensive inventory and mapping of all data assets, specifying the type of data being handled, including PII and sensitive data.
* Utilize a recognized privacy risk assessment framework to guide the risk assessment process.
* Document identified privacy risks in a list of potential risks, detailing the nature of the risk and potential impact.
 |
| Click or tap here to enter text. |
| 1. How does the organization ensure that your privacy risk assessments are comprehensive and up-to-date, specifically regarding handling PII and sensitive data? \*

Response Guidelines:* Conduct regular reviews and updates of the privacy risk assessment process to reflect changes in data processing activities and emerging threats.
* Engage cross-functional teams, including legal, IT (Information Technology), and compliance, to ensure a holistic approach to privacy risk assessment.
* Maintain detailed documentation of risk assessments and mitigation actions and review them periodically for accuracy and completeness.
 |
| Click or tap here to enter text. |

### **Protect**

The Protect domain in the NIST Privacy Framework is dedicated to implementing measures that ensure the confidentiality, integrity, and availability of personal data. This domain includes the deployment of technical and administrative controls to safeguard personal data against privacy breaches and other risks. By prioritizing the protection of personal data, organizations can mitigate privacy risks, comply with regulatory requirements, and maintain the trust of individuals and stakeholders.

| **NIST Privacy Framework – Open Ended Questions** |
| --- |
| 1. What technical and organizational measures have you implemented to protect personal data, including PII and sensitive data, from unauthorized access, disclosure, or misuse? \*

Response Guidelines:* Use encryption for data at rest and in transit to protect sensitive information.
* Implement strong access controls, including MFA and role-based access permissions.
* Conduct regular security audits and vulnerability assessments to identify and mitigate potential threats.
* Provide ongoing training and awareness programs to ensure employees understand their responsibilities in protecting personal data.
 |
| Click or tap here to enter text. |
| 1. How do you monitor and respond to potential privacy incidents or breaches, particularly those involving PII and sensitive data? \*

Response Guidelines:* Utilize real-time monitoring tools and intrusion detection systems to identify potential privacy incidents or breaches.
* Establish a dedicated incident response team to investigate and respond to any detected breaches promptly.
* Implement a clear incident response plan that includes steps for containment, mitigation, notification, and remediation.
* Conduct post-incident reviews to analyze the cause of the breach and implement measures to prevent future occurrences.
 |
| Click or tap here to enter text. |

### **Control**

The Control domain in the NIST Privacy Framework focuses on implementing appropriate safeguards to manage privacy risks. This domain includes the development and implementation of privacy controls, policies, and procedures that protect personal data and ensure compliance with privacy regulations. By effectively controlling privacy risks, organizations can prevent unauthorized access, use, or disclosure of personal data, thereby protecting individual privacy and maintaining trust.

| **NIST Privacy Framework – Open Ended Questions** |
| --- |
| 1. What measures and controls has the organization implemented to mitigate identified privacy risks, particularly those involving PII and sensitive data, and how do you evaluate their effectiveness? \*

Response Guidelines:* Implement encryption, access controls, and data masking to protect PII and sensitive data.
* Secure data centers with restricted access, surveillance, and environmental controls to protect physical data storage.
* Conduct regular audits, vulnerability assessments, and penetration testing to evaluate the effectiveness of implemented controls.
 |
| Click or tap here to enter text. |
| 1. How does your organization enforce privacy controls in day-to-day operations, particularly concerning the handling of PII and sensitive data? \*

Response Guidelines:* Restrict access to PII and sensitive data based on roles and responsibilities, using MFA and regular access reviews.
* Implement strict data handling procedures, including secure data transfer protocols and data minimization practices.
* Conduct regular training sessions programs to educate employees on data privacy, and proper handling of PII and sensitive data.
* Use monitoring tools and conduct regular audits to ensure compliance with privacy policies and identify potential breaches or areas for improvement.
 |
| Click or tap here to enter text. |

### **Communicate**

The Communicate domain in the NIST Privacy Framework emphasizes the importance of transparent communication regarding privacy practices and policies. This domain ensures that individuals are informed about how their data is collected, used, and protected. Effective communication fosters trust and enables individuals to make informed decisions about their personal data. By prioritizing transparency, organizations can enhance their reputation and build stronger relationships with stakeholders.

| **NIST Privacy Framework – Open Ended Questions** |
| --- |
| 1. How does your organization communicate its privacy practices and policies, especially those related to PII and sensitive data, to stakeholders, including employees, customers, and partners? \*

Response Guidelines:* Publish privacy policies and practices on the company website and make them easily accessible to all stakeholders.
* Conduct regular training sessions and workshops for employees to ensure they understand and adhere to privacy practices and policies.
* Include privacy policy information in customer and partner agreements, and provide clear, concise documentation during onboarding processes.
* Use newsletters, email updates, and internal communication platforms to keep all stakeholders informed about any changes or updates to privacy practices and policies.
 |
| Click or tap here to enter text. |
| 1. What mechanisms are in place for stakeholders to provide feedback or report concerns about privacy practices, specifically in relation to PII and sensitive data? \*

Response Guidelines:* Provide a dedicated privacy email address or hotline for stakeholders to report concerns or provide feedback.
* Implement an online feedback form on the company website to facilitate easy reporting of privacy issues.
* Establish a whistleblower policy that allows anonymous reporting of privacy concerns, ensuring protection for those who report.
* Conduct regular surveys and feedback sessions with stakeholders to gather input on privacy practices and identify areas for improvement.
 |
| Click or tap here to enter text. |

## **Risk Assessment Supplemental Questions**

|  |
| --- |
| 1. How many distinct electronic records do you retain that include any of the information types specified below? \*

If a record fits into multiple categories, count it in the most appropriate one. |
| Personally Identifiable Information (PII) | Click or tap here to enter text. |
| Payment Card Information (PCI) | Click or tap here to enter text. |
| Protected Health Information (PHI) | Click or tap here to enter text. |
| Biometric Information | Click or tap here to enter text. |
|  |
| 1a. Is all such information encrypted in transit and at rest?  | Yes[ ]  | No[ ]  |
| 1b. Do you retain paper copies of any of these records on your business premises? | Yes[ ]  | No[ ]  |

|  |
| --- |
| 1. Do you have any end-of-life hardware, end-of-support software, or obsolete applications on your network?
 | Yes[ ]  | No[ ]  |
| 2a. If “Yes”, please list all devices, software, and applications? | Click or tap here to enter text. |
| 2b. If “Yes”, is it segregated with compensating controls?  | Click or tap here to enter text. |
| 2c. If “Yes”, do you have a replacement plan? | Click or tap here to enter text. |
| 2d. If “No”, what are the obstacles preventing replacement? | Click or tap here to enter text. |

|  |
| --- |
| 1. Does your agency have an incident response plan (IRP) to cover all cyber risk exposures (e.g., cloud applications, on-prem network, and user access)?
 | Yes[ ]  | No[ ]  |
|  3a. If “No” specify what facets/risks are not addressed. |
| Click or tap here to enter text. |
|  |
| 1. Is the plan updated after every significant change to your operating environment?
 | Yes[ ]  | No[ ]  |

|  |
| --- |
| 1. Does your agency have a Business Continuity Plan (BCP) and Disaster Recovery Plan (DRP) for all mission critical operations?
 | Yes[ ]  | No[ ]  |
|  5a. If “No” specify what operations are not included in the plan. |
| Click or tap here to enter text. |
|  |
| 1. Is the plan updated after every significant change to

 your operating environment?  | Yes[ ]  | No[ ]  |

|  |
| --- |
| 1. Does your agency patch zero day and critical vulnerabilities, including any required reboots, within 24 hours of receiving a notification?
 | Yes[ ]  | No[ ]  |
| 1. Does your agency patch all other vulnerabilities,

 including any required reboots, within 30 days of  receiving a notification?  | Yes[ ]  | No[ ]  |

|  |
| --- |
| 1. Do you enforce MFA for all login requirements of your operations?
 | Yes[ ]  | No[ ]  |
|  9a. If “No,” specify what login functions are not protected by MFA. |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Do you have private Wi-Fi at any of your agency locations?
 | Yes[ ]  | No[ ]  |
|  10a. When was it last subjected to penetration testing? |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Do you have public Wi-Fi at any of your agency locations?
 | Yes[ ]  | No[ ]  |
|  11a. When was it last subjected to penetration testing? |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Is your public or private Wi-Fi connected to your internal network?
 | Yes[ ]  | No[ ]  |

|  |
| --- |
| 1. What is your agency’s total annual budget (Include only general funds. Exclude federal funding, special funds and grants)?
 |
| Click or tap here to enter text. |
| 1. What is your agency's total annual IT operating budget?
 |
| Click or tap here to enter text. |
| 1. What is your agency’s total annual IT security budget?
 |
| Click or tap here to enter text. |
| 1. How many authorized users have access to your agency’s network?
 |
| Click or tap here to enter text. |
|  16a. How many of these are privileged account users?  |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Do you allow remote access to your network by employees, contractors, or others?
 | Yes[ ]  | No[ ]  |
| 1. Do you allow remote access to your network through non-state-owned devices?
 | Yes[ ]  | No[ ]  |

|  |
| --- |
| 1. What is the total count of the following assets? Include all items in inventory or depreciable assets if no inventory exists:
 |
| Desktops/Laptops: | Click or tap here to enter text. |
| Tablets: | Click or tap here to enter text. |
| Physical Servers | Click or tap here to enter text. |
| Virtual Servers  | Click or tap here to enter text. |
| Fax/Printers | Click or tap here to enter text. |
| Other | Click or tap here to enter text. |
| Please describe any assets listed as “Other”: |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Do you have an asset management system?
 | Yes[ ]  | No[ ]  |
| 1. Has your agency implemented artificial intelligence (AI) tools or products in its IT environment?
 | Yes[ ]  | No[ ]  |
|  21a. If “Yes”, have you completed any AI risk  assessments? | Yes[ ]  | No[ ]  |
| 21b. If “Yes”, do you have security policies and procedures for AI? | Yes[ ]  | No[ ]  |
| 1. Have you implemented any AI risk assessments?
 | Yes[ ]  | No[ ]  |
| 1. What AI applications are used?
 |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Does your agency conduct monthly authenticated scans on your network?
 | Yes[ ]  | No[ ]  |
| 24a. If “No” what is the agency timeline to be onboarded to authenticated scanning? |
| Click or tap here to enter text. |

|  |
| --- |
| 1. Are there any other cybersecurity questions or concerns that you would like to share confidentially with the CSO?
 |
| Click or tap here to enter text. |

**The last two questions of this assessment survey require responses in the Response Worksheet attached to the email notifying you of this assessment. Once completed, please submit the completed Response Worksheet in Part 2: Supplemental Questions.**

|  |
| --- |
|  |
| 1. Identify all hosted applications in the table below. As applicable, indicate by checking the appropriate box whether the application stores PII, PCI, PHI or security/sensitive information.

*See Examples Below* |
| Application Name  | IP/URL  | Hosted On  | PII (Yes/No) | PCI (Yes/No) | PHI (Yes/No) | Security/Sensitive Info (Yes/No) | Physical Location  |
| *ExampleApp1*  | [*https://example1.com*](https://example1.com/) | *Example Host* | *Yes*  | *Yes*  | *Yes*  | *Yes*  | *Cloud* |
| *ExampleApp2*  | [*https://example2.com*](https://example2.com/) | *Private DOIT Host* | *No* | *No* | *No* | *No* | *On-Prem* |
| *ExampleApp3*  | [*https://example3.com*](https://example3.com/) | *AWS* | *Yes* | *Yes* | *Yes* | *Yes* | *Cloud* |

Notes:

* PII: Personally Identifiable Information (e.g., names, email addresses).
* PCI: Payment Card Information.
* PHI: Protected Health Information (e.g., health records).
* Security/Sensitive Info: Data like authentication credentials, internal security policies, encryption keys, or proprietary business data.

Additional Details:

* Cloud-based Applications: Ensure to get a comprehensive list from your cloud service provider’s dashboard or documentation.
* DoIT Private Cloud: Verify with the internal IT team for accurate URLs and physical locations.
* On-Prem Servers: Check with the IT team for the specific locations of servers within your organization.

|  |
| --- |
| 1. Identify all Operational Technology (OT) and Internet of Things (IoT) in your environment (including security cameras, badged access, etc.):

*See Examples Below* |
| Type  | Device/  Technology | Description | Segmented (Yes/No)  | Visible from Public Internet (Yes/No)  | Policies and Controls  | URL/IP Address  |
| *OT*  | *Security Cameras*  | *IP cameras for monitoring premises*  | *Yes* | *No* | *Regular security reviews, access controls*  | *ExampleURL.com* |
| *OT*  | *Badged Access System*  | *Electronic entry system for buildings*  | *No* | *Yes* | *Access control policies, encryption of data*  | *123.456.7891* |
| *OT*  | *Fire Control System*  | *Monitors and manages fire alarms*  | *No* | *Yes* | *Incident response plan, system audits*  | *123.456.7891* |

Notes:

* Segmented: Indicates whether OT and IoT systems are isolated from IT environments to enhance security.
* Visible from Public Internet: Indicates whether the device or system is accessible from the public internet, which may pose additional security risks.
* Policies and Controls: Include any relevant security measures and protocols that are in place to protect each device or system.