Annual Cybersecurity Office Risk Assessment FY25

Introduction

The rising threat of cybersecurity breaches and hacks necessitates that state entities strengthen their defenses to safeguard sensitive information and critical infrastructure. This assessment, based on the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, provides an enterprise-wide view of the current cybersecurity posture of state entities and ensures adherence to the directives specified in **Executive Order 2024-011**.

Executive Order 2024-011

The Executive Order specifies that state entities take the following actions to ensure compliance with NIST standards: They must adopt and implement cybersecurity, information security, and privacy policies, standards, and procedures based on a moderate-impact security control baselines, frameworks, and standards issued by NIST.

The 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.

Confidentiality Notice

Data collected in this survey that could reveal a specific vulnerability in an information technology system and that is identified as “cybersecurity sensitive” by the responder or assessed to be “cybersecurity sensitive” by the Cybersecurity Office (CSO), is exempt from disclosure pursuant to an Inspection of Public Records request and will not be disclosed in response to any such request. Also, the CSO will follow principles of least privilege and need-to know in sharing this information internally and with initiative stakeholders and supporting vendors.

Submission

After you submit the responses to this survey, your agency leader and IT lead will receive an e-mail prompting each of them to review the survey responses and certify the submission in Docusign. The survey process is not complete until both the agency leader and the IT lead have certified the responses in Docusign. If a required signatory wants to change a response to any question in the survey, the agency must contact NMCybersecurity@cyber.nm.gov and ask to have the survey reset. This will reset all questions and require the agency to answer each of them again. After the CSO receives a fully executed certification, it will provide an assessment report to the agency. The agency will use the assessment report to provide the certification, or exemption request, contemplated by Executive Order 2024-11.

What to Expect

The assessment is divided into two parts, the **Cybersecurity Risk Assessment** and **Risk Assessment Supplemental Questions**.

Part 1 - Cybersecurity Risk Assessment:

The assessment survey is broken down into the six control groups dictated in NIST CSF 2.0 which includes:

- Govern
- Identify
- Protect
- Detect
- Respond
- Recover

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.

Part 2- Risk Assessment Supplemental Questions:

The last two Supplemental Questions require responses in the below worksheet.

Response Worksheet

Once the **Response Worksheet.xlsx** is completed, save as a **PDF** and attach to the end of the **Risk Assessment Supplemental Questions MS Forms (Question 57)**

Submission:

All Cybersecurity Risk Assessments and supplemental questions are to be **completed *and* submitted by *October 10, 2024***.

It is ***strongly*** recommended that you **first** complete the consolidated static Microsoft Word document (embedded below) and **then** transfer answers to their respective Microsoft Forms links. There is functionality to save progress within Forms, but to avoid losing any answers and any progress we recommend also recording responses manually.

Cybersecurity Risk Assessment Form

However, both the **Cybersecurity Risk Assessment** and **Risk Assessment Supplemental Questions** responses ***must be*** formally submitted to the Cybersecurity Office via their respective **Microsoft Forms** links below:

- Submit **Cybersecurity Risk Assessment** responses here
- Submit **Risk Assessment Supplemental Questions** responses here

The following sections contain examples of how the questions will be posed in the form and Microsoft Forms.

Scoring Format

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.

Microsoft Forms Assessment Survey – Examples

Here is an example of a question using the scale above that you will see in the assessment:

15. **Policies, Procedures, and Processes** *

	0	1	2	3	4	5	N/A
The entity establishes, communicates, and enforces cybersecurity policies, procedures, and processes, and regularly reviews and updates them to ensure they remain effective and current.	◯	◯	◯	◯	◯	◯	◯

Please note, if you choose **N/A**, you are required to explain why in the corresponding field at the bottom of the question bank. The required explanation field is shown below:

16. **If you selected "N/A" to any of the questions above, please explain below:**

Enter your answer

Here is an example of a Free Response Question you will see in the assessment:

17. 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.

*

Please enter at least 30 characters

Assessment Survey Form - Examples

Entities that wish to collaborate may use the Microsoft Word version of the assessment. The Word version contains all the same questions and content as the Microsoft Forms version. The Word version of the assessment is recommended for larger entities or entities that wish to collaborate on the assessment.

Here is an example of the Word version of the assessment:

Policies, Procedures, and Processes*

	0	1	2	3	4	5	N/A
The entity establishes, communicates, and enforces cybersecurity policies, procedures, and processes, and regularly reviews and updates them to ensure they remain effective and current.	☐	☐	☐	☐	☐	☐	☐

Please note, if you choose Not Applicable, you are required to explain why in the corresponding field at the bottom of the question bank. The required explanation field is shown below:

current.

If you selected "N/A" to any of the questions above, please explain below:

Click or tap here to enter text.

Here is an example of a Free Response Question you will see in the Word assessment:

Policies, Procedures, and Processes – Open Ended Questions

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.

Glossary

Term	Definition
Access Control	Mechanisms that restrict access to information systems and data to authorized users and processes.
Adverse Event	An event that negatively impacts the security, availability, or integrity of an organization's information systems.
Artificial Intelligence	Refers to systems performing functions with minimal human input. For instance, managing licensing is AI, but analyzing data for decision-making is not.
Asset	An asset is any data, device, or other component of an organization's environment that supports information-related activities.
Asset Management	The process of inventorying and managing an organization's assets, including data, hardware, software, systems, and facilities.
Audit	A systematic evaluation of an organization's systems, processes, and controls to ensure compliance with policies, standards, and regulations.
Authentication	The process of verifying the identity of a user, device, or process.
Authenticated Scans	Security scans conducted with valid credentials to provide a more comprehensive assessment of vulnerabilities within a system, often revealing issues that unauthenticated scans might miss.
Authorization	The process of granting or denying access to resources based on the verified identity.
Baseline	A set of conditions or standards used as a reference point for measuring performance or compliance.
Business Continuity Plan (BCP)	A plan that outlines how an organization will continue operating during and after a disruption.
Business Environment	The combination of internal and external factors that influence an organization's operations, including its cybersecurity posture.
Compliance Obligations	Legal, regulatory, and contractual requirements that an organization must adhere to.
Containment	Actions taken to limit the impact of a cybersecurity incident and prevent further damage.
Critical Functions	Essential activities or processes that are vital to the operation of an organization.
Criticality	The importance of an asset or process to the functioning of an organization.
Critical / High-Risk Vulnerabilities	Are security weaknesses in your environment that could lead to severe consequences if exploited, such as unauthorized access to sensitive data, system compromise, or major operational disruptions.

Term	Definition
Cyber Incident	An event that may indicate that an organization's systems or data have been compromised.
Cybersecurity Dependencies	Relationships between systems, processes, or organizations that impact cybersecurity.
Cybersecurity Risk Management	The process of identifying, assessing, and mitigating risks to an organization's information systems and data.
Cybersecurity Strategy	A plan that outlines how an organization will protect its information systems and data from cybersecurity threats.
Data Backup	The process of creating copies of data to ensure its availability in case of loss or corruption.
Data Dictionary	A centralized repository of information about data, such as meaning, relationships to other data, origin, usage, and format.
Data Flow	The movement of data within and between systems.
Data Leak	The unauthorized transmission of data from within an organization to an external destination.
Data Security	Measures taken to protect data from unauthorized access, alteration, or destruction.
Detection	The process of identifying potential cybersecurity incidents through monitoring and analysis.
Detection Mechanisms	Tools and processes used to identify potential cybersecurity incidents.
Encryption	The process of converting data into a coded form to prevent unauthorized access.
End of Life / End of Support / Obsolete	Refers to hardware or software no longer receiving updates or patches from the manufacturer, regardless of depreciation.
Enterprise Risk Management (ERM)	A comprehensive approach to identifying, assessing, and managing risks across an organization, including cybersecurity risks.
External Exposures	Refers to vulnerabilities or weaknesses in your systems that are accessible/visible from outside your network, potentially allowing unauthorized external parties to exploit them.
External Network Connections	Connections between an organization's internal network and external networks, such as the internet.
Governance	The framework of policies, roles, responsibilities, and processes that guide an organization's cybersecurity efforts.
Governance Framework	The structure of policies, roles, responsibilities, and processes that guide an organization's cybersecurity efforts.

Term	Definition
Human Resources Practices	Procedures related to the management of personnel, including hiring, training, and termination.
Identity Management	The process of identifying, authenticating, and authorizing users and devices.
Incident	An event that has been verified through investigation and analysis to be a genuine security breach or attack impacting the confidentiality, integrity, or availability of information systems or data.
Incident Recovery	The process of restoring systems and data after a confirmed cybersecurity incident.
Incident Response	The actions taken to address and manage the aftermath of a cybersecurity incident.
Incident Response Plan	A documented plan that outlines the steps an organization will take to respond to a cybersecurity incident.
Incident Triage	The process of prioritizing incidents based on their severity and impact on the organization.
Indicators of Compromise (IoC)	Observable artifacts or behaviors that indicate a potential security breach.
Integrity	The assurance that data is accurate, complete, and has not been altered in an unauthorized manner.
Integrity Checking Mechanisms	Tools and processes used to verify the integrity of software, firmware, and information.
Least Privilege	A principle that restricts users' access rights to only what is necessary for them to perform their job functions.
Mitigation	Actions taken to reduce the severity or impact of a cybersecurity incident.
Mitigation Plan	Is a detailed strategy outlining the steps taken to reduce or eliminate the risks associated with vulnerabilities or exposures. It includes actions to address the issue, responsible parties, and timelines for implementation.
Monitoring	The continuous observation of systems and networks to detect potential cybersecurity incidents.
Network Monitoring	The continuous observation of network traffic to detect anomalies and potential security incidents.
Network Segmentation	The practice of dividing a network into smaller segments to improve security and performance.
Periodic Process	A recurring process conducted regularly to ensure ongoing compliance and effectiveness.
Point of Contact (POC)	The designated individual responsible for managing and communicating about cybersecurity within an organization.

Term	Definition
Policies, Procedures, and Processes	The documented guidelines and steps that an organization follows to manage cybersecurity risks.
Privacy Policies	Guidelines that dictate how an organization collects, uses, and protects personal data.
Record	A distinct data set that compiles information pertaining to an individual or transaction. "Record" does not mean each individual file or document that contains protected information, unless an individual file or record constitutes a distinct data set. For example, a patient file would constitute a single record, even if the file contains multiple instances of PHI. Conversely, each transaction that generated PCI would constitute a separate record, even if all of the PCI data is maintained in a single file or data set. This definition is intended to enable the OCS to ascertain how many distinct individuals could potentially be impacted by a data breach and should be interpreted in light of that objective.
Recovery	The process of restoring normal operations after a cybersecurity incident.
Resilience	The ability of an organization to adapt to and recover from cybersecurity incidents while maintaining critical operations.
Restoration	The process of returning systems and data to their normal state after a cybersecurity incident.
Risk Appetite	The amount and type of risk an organization is willing to accept in pursuit of its objectives.
Risk Assessment	The process of identifying, evaluating, and prioritizing risks to an organization's information systems and data.
Risk Management Strategy	A plan that outlines how an organization will manage and mitigate risks to its information systems and data.
Risk Response	Actions taken to address identified risks, including mitigation, acceptance, transfer, or avoidance.
Risk Tolerance	The acceptable level of variation in performance relative to the achievement of objectives.
Roles and Responsibilities	The specific duties and obligations assigned to individuals or groups within an organization to manage cybersecurity risks.
Security / Sensitive Information	Refers to data that, if disclosed or compromised, could potentially harm the security, confidentiality, or integrity of an organization or individual. This includes, but is not limited to, authentication credentials, internal security policies, encryption keys, or proprietary business data.
Security Controls	Safeguards or countermeasures to avoid, detect, counteract, or minimize security risks.

Term	Definition
Security Tests	Evaluations conducted to assess the effectiveness of security controls and identify vulnerabilities.
Separation of Duties	A principle that divides tasks and responsibilities among multiple individuals to reduce the risk of fraud or error.
Stakeholder Communication	The process of informing and engaging individuals or groups that have an interest in an organization's cybersecurity efforts.
Stakeholders	Individuals or groups that have an interest in an organization's cybersecurity efforts, including internal and external parties.
Supply Chain Risk Management	The process of identifying, assessing, and mitigating risks associated with third-party suppliers and partners.
Third-Party Risk	The potential risks associated with external entities that have access to or impact an organization's information systems.
Third-Party Stakeholders	External entities, such as suppliers, customers, and partners, that have a relationship with an organization and may impact its cybersecurity posture.
Threat	Any circumstance or event with the potential to adversely impact organizational operations, assets, or individuals.
Threat Analysis	The process of examining potential threats to determine their likelihood and impact on the organization.
Threat Landscape	The overall environment of potential threats that an organization faces.
Vulnerability	A weakness in a system, process, or control that can be exploited by a threat.
Vulnerability Disclosure	The process of reporting identified vulnerabilities to the responsible parties for remediation.