Maryland

DEPARTMENT OF
INFORMATION TECHNOLOGY

Office of Security Management

STATE MINIMUM CYBERSECURITY STANDARDS

BEST PRACTICES GUIDEBOOK

Version 1.0

Date Issued: May 10, 2024

Date Last Revised:

Maryland Government
Department of Information Technology
100 Community Place
Crownsville, MD 21032

Table of Contents

List of Tables and Figures

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

Revision Control History

Date	Reason for Change	Changed by	Version
05/10/2024	CSF Guidebook	Netta Squires	1

Table 1: Revision Control History

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

1. Executive Summary

Per Section 5 of SB754, of 2022, on or before June 30, 2023, each unit of local government was required to certify to the DoIT Office of Security Management ("OSM") compliance with State minimum cybersecurity standards. The certification was to be reviewed by independent auditors, and any findings must be remediated. For findings pertaining to State cybersecurity standards not remediated by July 1, 2024, The DoIT Office of Security Management is to provide guidance for the unit to achieve compliance with the cybersecurity standards.

2. Purpose

To support the Executive Branch agencies and local jurisdictions, this guidebook was developed to provide best practices for compliance with the State Minimum Cybersecurity Standards, 2022 (SMCS). This document should not be viewed as an authoritative policy, but as a foundation for how to develop cybersecurity maturity.

3. Scope

The scope of this guidance is explicit to the controls identified in the NIST CSF version 1.1. Each control is accompanied by the State Minimum Cybersecurity Standard CMMI score.

4. Authority

- Section 5 of SB754, Ch. 241 (2022)
- Section 5 of SB812, Ch. 242 (2022)

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

5. Definitions & Acronyms

All defined terms below should be capitalized within the document and defined below.

Acronym/Phrase	Definition
CSF	Cybersecurity Framework, published by NIST
CMMI	Cybersecurity Maturity Model Integration
DoIT	Maryland Department of Information Technology
NCSR	National Cybersecurity Review
NIST	National Institute of Standards and Technology
OSM	Office of Security Management
SMCS	State Minimum Cybersecurity Standards

Table 2: Definitions & Acronyms

6. Standards

The State of Maryland's Minimum Cybersecurity Standards align to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), consisting of controls that contribute to an organization's overall cybersecurity maturity while mitigating or reducing cybersecurity risk and vulnerabilities. The controls below are subject to change and represent the "State Minimum Cybersecurity Standards". Independent audit or 3rd party assessment must validate that each control meets a minimum Cybersecurity Maturity Model Integration (CMMI) maturity score of at *least* a "1" (meaning "Initial" or "Performed") or a "2" (meaning "Managed"), depending on the control.

A score of "**1**" indicates that the control is **performed** by the organization in an ad-hoc fashion without consistency or documentation. A score of "**2**" indicates the control is **performed consistently with supporting documentation** such as written plans, procedures, or standards. To certify compliance, units of State Government must meet the minimum required CMMI maturity scores for each NIST CSF control in sections below.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

6.1 Identify (ID) Controls

Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities

- **ID.AM - Asset Management:** Organizations assess, prioritize, and oversee assets based on their relevance to business objectives and risk management approaches.
  - **ID.AM-1:** Physical devices and systems within the organization are inventoried.
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Keep the list of devices and systems up to date by regularly adding, removing, upgrading, or moving them, and consider using automated tools like network scanners to help with this.
    - Tag and record all the gadgets and machines in the company, like computers, servers, and IoT devices, with unique details such as make, model, and location.
    - Set up a system to keep an eye on how physical devices are used and their status, including tracking software changes and hardware setups, and use monitoring tools to spot any unauthorized activities.
    - Create a system to monitor physical device usage, track software and hardware changes, and use monitoring tools to detect unauthorized activities.

  - **ID.AM-2:** Software platforms and applications within the organization are inventoried
  - **State Min Requirement:** 1
  - **Best Practices:**
    - List and identify all software used in the organization, covering operating systems, productivity tools, communication software, and any other applications across the company's systems.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Understanding the software in use, aids in evaluating security risks for each platform and application, enabling organizations to prioritize critical security measures.
- Track software licenses for each platform and app to ensure legal compliance, including details like the number of licenses, expiration dates, and permitted usage.

- **ID.AM-3:** Organizational communication and data flows are mapped
- **State Min Requirement:** 1
- **Best Practices:**
  - Understanding how data moves within its systems, which systems it interacts with, and where sensitive information is stored or sent is essential for the organization.
  - Document all communication channels like emails and messaging apps to spot data risks.
  - Maintain regular reviews and updates of the communication and data flow map to adjust to changes in technology or processes, ensuring accuracy and effective response to cybersecurity threats.

- **ID.AM-4:** External information systems are catalogued
- **State Min Requirement:** 1
- **Best Practices:**
  - Identify all external systems accessing organization data, including cloud services, vendors, and partner networks.
  - Document characteristics of each external system, like purpose and security measures, to assess risks and ensure proper security.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Regularly update and monitor the catalog of external systems to adapt to changes and identify security risks.

- **ID.AM-5:** Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value
- **State Min Requirement:** 1
- **Best Practices:**
  - Determine the protection needs of resources by classifying them according to sensitivity, importance, or regulatory requirements.
  - Assess each resource to determine its importance to the organization, considering factors like its impact on business operations, finances, and reputation if compromised.
  - Determine the business value of resources to prioritize those essential for meeting organizational goals and providing value to stakeholders.

- **ID.AM-6:** Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
- **State Min Requirement:** 1
- **Best Practices:**
  - Identify and define cybersecurity roles for everyone in the organization, including third-party partners, clarifying who is responsible for tasks like data protection and incident response.
  - Ensure effective communication of identified roles to ensure everyone comprehends their responsibilities in cybersecurity and risk management.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Implement training programs to inform all about cybersecurity roles and best practices for protecting data and systems.
- Keep cybersecurity roles aligned with the organization's changing structure and technology landscape by regularly reviewing and updating them.

- **ID.BE - Business Environment:** The organization considers its mission, stakeholder expectations, and legal/regulatory obligations when assessing and managing cybersecurity risks.
  - **ID.BE-2:** The organization's place in critical infrastructure and its industry sector is identified and communicated
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Identify the primary industry sector to which the organization belongs, such as healthcare or finance, as distinct regulations and standards apply to each sector.
    - Assess whether the organization relies on or supports critical infrastructure, such as power grids and communication networks; even if not directly involved, supplying them might make the organization a target.
    - Share the organization's industry classification and critical infrastructure dependencies with relevant personnel, including leadership, IT security teams, and risk management, to tailor cybersecurity measures to address specific threats.

  - **ID.BE-3:** Priorities for organizational mission, objectives, and activities are established and communicated
  - **State Min Requirement:** 2

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **Best Practices:**
  - Define the organization's core purpose (mission) and objectives to clarify what requires protection.
  - List essential functions and processes that keep the organization running, as they are the priorities for cybersecurity efforts.
  - Share the organization's mission, objectives, and key activities with everyone involved to help them understand how cybersecurity protects their work.

- **ID.BE-4:** Dependencies and critical functions for delivery of critical services are established
- **State Min Requirement:** 2
- **Best Practices:**
  - Identify the essential services provided by the organization, like processing customer payments and managing patient data.
  - Identify the systems and processes that each critical service relies on to function, similar to mapping the electrical wires powering essential equipment.
  - Focus cybersecurity efforts on safeguarding critical services and the systems they depend on, prioritizing resources on what matters most.

- **ID.BE-5:** Resilience requirements to support delivery of critical services are established
- **State Min Requirement:** 2
- **Best Practices:**
  - Plan for disruptions by identifying potential threats that could affect critical services, such as cyberattacks, power outages, or natural disasters, to develop mitigation plans.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Establish acceptable downtime for critical services to determine how quickly recovery should occur following a disruption.
- Outline actions to restore critical services after a disruption, which may include backups, redundancy measures, or disaster recovery plans.

- **ID.GV- Identify Governance:** The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored to align with the organization's overall mission and business objectives.
  - **ID.GV-1:** Organizational information security policy is established and communicated
  - **State Min Requirement:** 2
  - **Best Practices:**
    - Develop a clear and concise written information security policy outlining the organization's cybersecurity approach.
    - Publish the information security policy in a central location accessible to everyone, such as a company intranet, shared document platform, or printed copies.
    - Educate employees about the information security policy through training sessions, awareness campaigns, or including it in new hire onboarding processes.

  - **ID.GV-2:** Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
  - **State Min Requirement:** 1
  - **Best Practices:**

- Clarify cybersecurity roles and responsibilities for internal staff, encompassing IT security teams, department heads, and regular employees, ensuring everyone understands their obligations in cybersecurity.
- Identify external vendors, cloud service providers, or third-party suppliers that handle data or access.
- Establish clear expectations for external partners' cybersecurity practices, which may include requiring them to meet specific security standards or outlining data security protocols.

- **ID.GV-3:** Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
- **State Min Requirement:** 1
- **Best Practices:**
  - Identify the laws and regulations relevant to the organization's cybersecurity practices and data handling, which may encompass industry-specific regulations or broader privacy laws.
  - Understand the types of data collected, stored, and processed to determine applicable regulations and ensure secure data management. - Compare current practices with legal requirements to identify gaps and implement procedures to address them, which may involve creating data access controls or updating privacy policies.
  - Keep informed about changes in legal and regulatory requirements by regularly reviewing the applicable laws and updating the compliance plan accordingly.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **ID.RA- Risk Assessment:** The organization prioritizes the assessment and mitigation of cybersecurity risks to protect its assets and individuals.
    - **ID.RA-1:** Asset vulnerabilities are identified and documented
    - **State Min Requirement:** 1
    - **Best Practices:**
        - Create a list of all devices, software, applications, and data, like taking stock of everything valuable owned.
        - Use vulnerability scanning tools to find potential security weaknesses in assets, like having tools check locks and alarms for vulnerabilities.
        - Record identified vulnerabilities and their severity levels to prioritize addressing the most critical weaknesses first, like keeping a log of security issues in the inventory.

    - **ID.RA-2:** Cyber threat intelligence is received from information sharing forums and sources
    - **State Min Requirement:** 1
    - **Best Practices:**
        - Discover credible information-sharing forums and threat intelligence feeds relevant to the industry, like those provided by government agencies, security vendors, or industry consortia.
        - Locate trusted information-sharing forums and threat intelligence feeds pertinent to the industry, which may include sources from government agencies, security vendors, or industry groups.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Share the collected threat intelligence with the security team to update defenses and pinpoint potential vulnerabilities in systems.

- **ID.RA-3:** Threats, both internal and external, are identified and documented
- **State Min Requirement:** 1
- **Best Practices:**
  - Adopt a hacker's mindset and brainstorm potential harm to the organization, including data breaches, malware attacks, insider threats (both accidental or malicious employee actions), and external threats (hackers, cybercriminals).
  - Research common threats relevant to the industry by reviewing industry reports, news articles, and cybersecurity resources for valuable insights.
  - Record all identified threats, detailing their potential impact on the organization, as this documented threat list serves as a vital reference for developing cybersecurity strategy.

- **ID.RA-4:** Potential business impacts and likelihoods are identified
- **State Min Requirement:** 1
- **Best Practices:**
  - Gather to identify possible security threats the organization could encounter, such as hacking, data breaches, or malware attacks.
  - Evaluate the potential consequences to the business for each threat, such as financial losses, reputational harm, or service disruptions.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Assign a likelihood rating to each threat, determining whether it's highly likely, somewhat likely, or unlikely to happen, in order to prioritize attention to the most critical threats.

- **ID.RA-5:** Threats, vulnerabilities, likelihoods, and impacts are used to determine risk
- **State Min Requirement:** 1
- **Best Practices:**
  - List potential security incidents that could harm the organization, such as data breaches, malware attacks, or denial-of-service attacks.
  - Identify vulnerabilities in systems and processes that could be exploited for each threat, such as outdated software, weak passwords, or lack of employee training.
  - Evaluate the risk by considering how likely each threat-vulnerability combination is to happen and its potential impact, aiding in prioritizing which security risks to address first.

- **ID.RA-6:** Risk responses are identified and prioritized
- **State Min Requirement:** 1
- **Best Practices:**
  - Keep a list of potential cybersecurity threats and vulnerabilities that could affect the organization, including both internal and external threats such as malware, phishing attacks, or human error. - Assess the potential damage of each threat and vulnerability, considering financial loss, reputational damage, and disruption to critical services. - Calculate a risk score by combining the likelihood of a threat occurring with its potential

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

impact, then prioritize addressing the highest-risk threats first to mitigate critical issues.

- **ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stake holders
- **State Min Requirement:** 1
- **Best Practices:**
  - Engage key stakeholders from various departments, such as IT, management, and legal, in shaping the risk management process to ensure everyone comprehends the plan and is committed to its success.
  - Document the risk management process clearly, including roles, responsibilities, and reporting procedures, and make sure stakeholders can easily access this information.
  - Arrange consistent meetings with stakeholders to review identified risks, mitigation strategies, and the effectiveness of risk management, keeping everyone informed and facilitating necessary adjustments.

- **ID.RM-2:** Organizational risk tolerance is determined and clearly expressed
- **State Min Requirement:** 1
- **Best Practices:**
  - Leadership needs to evaluate how much risk is acceptable by comparing the potential cost of security incidents to the cost of preventive measures.
  - Verify whether the organization depends on or assists critical infrastructure, like power grids or water treatment facilities. Supporting critical infrastructure, even indirectly, could attract threats.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Record the industry classification and critical infrastructure dependency, and then distribute this information to relevant personnel, such as leadership, IT security teams, and risk management, to tailor cybersecurity measures to particular threats.

- **ID.RM-3:** The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis
- **State Min Requirement:** 1
- **Best Practices:**
  - Study and comprehend typical cybersecurity threats within the industry sector to assess the level of risk that must be tolerated.
  - Consider the potential results of a successful cyberattack if the organization is critical infrastructure or supports it, such as widespread service disruptions, risks to public safety, or economic harm. Critical infrastructure might not accept higher risks because of these possible consequences.
  - Check industry-specific cybersecurity regulations to ensure alignment between risk tolerance and compliance requirements.

6.2 Protect (PR) Controls

Enables the capability to protect those assets in order to reduce the probability and consequences of negative cybersecurity incidents, while also enhancing the probability and consequences of capitalizing on opportunities.

- **PR.AC:** Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and for authorized devices, users and processes
- **State Min Requirement:** 2
- **Best Practices:**
  - Create a list of user accounts by department and geographical local (complete list of everybody who has access to the network).
  - Verify identity and issue credentials for each person.
  - Review applications and databases used by each department (application portfolio list of application and database used by department. Configuration database, people, question, or modifications CSV).
  - Audit or authorize devices users' processes: this requires identity and access management or an access management procedure to be written to put into place.

- **PR.AC-2:** Identities are proofed and bound to credentials based on the context of interactions
- **State Min Requirement:** 2
- **Best Practices:**
  - Restrict access to protect the physical access of the servers and data centers to only operations staff.
  - Verify a person's claimed identity at enrollment time using government-issued identity credentials (e.g., passport, visa, driver's license).
  - Label, physically, authorized hardware with an identifier for inventory and servicing purposes.

- **PR.AC-3:** Identities are proofed and bound to credentials based on the context of interactions
- **State Min Requirement:** 2
- **Best Practices:**

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Request multifactor authentication.
- Enforce policies for the minimum strength of passwords, PINs, and similar authenticators.
- Reauthenticate periodically users, services, and hardware based on risk (e.g., in zero trust architectures).
- Ensure that authorized personnel can access accounts essential for protecting safety under emergency conditions.
- Use VPNs for secure remote access.

- **PR.AC-4:** Access permissions are managed, incorporating the principles of least privilege and separation of duties
- **State Min Requirement:** 2
- **Best Practices:**
  - Ensure that Human resources engage with the hiring manager to include it in job descriptions that meet access standards. Bernard Institute.
  - Protect identity assertions used for single sign-on and federated system authentication and user information.
  - Use standards-based identity claims in all situations and follow all advice for generation (data models, metadata), protection (digital signing, encryption), and verification (signature validation).

- **PR.AC-5:** Network integrity is protected, incorporating network segregation where appropriate
- **State Min Requirement:** 1
- **Best Practices:**
  - Create a topology of infrastructure WAN, LAN and VLANS (show where all the devices and data centers are located).
  - Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health).
- Restrict access and privileges to the minimum necessary (e.g., zero trust architecture). Review periodically the privileges associated with critical business functions to confirm proper separation of duties.

- **PR.AC-6:** Identities are proofed and bound to credentials and asserted in interactions
- **State Min Requirement:** 1
- **Best Practices:**
  - Validate the credentials for all new hires.
  - Approved that the new hires are going to work on the network
  - Ensure that whatever the access control is that we give the new hires a token maybe it's a user account that can be proved where they go in the organization. A record can be created from them.
  - Proof bound to credentials in the directions so we have people will give them access to perform a job on the on the network for business.
  - Employ additional physical security controls for areas that contain high-risk assets. For example, escort guests, vendors, and other third parties within areas that contain business-critical assets.

- **PR.AC-7:** Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).
- **State Min Requirement:** 1
- **Best Practices:**

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Analyze current user and device authentication systems.
- Create access control architecture to display organization segmentation.
- Create a digital trail around your company's work.
- Install host-based firewalls and endpoint security devices.
- Standardize device setups and carefully manage modifications.
- Disable device services and functionalities that are not mission-critical.
- Use single- or multi-factor authentication, based on context, for organization and set situation-specific authentication requirements.
- Consider the sensitivity of the data or system being accessed.
- Reduces spoofing and repudiation risks.

- **PR.AT:** Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.
  - **PR.AT-1:** All users are informed and trained
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Provide basic cybersecurity awareness and training to employees, contractors, partners, suppliers, and all other users of the organization's non-public resources.
    - Train personnel to recognize social engineering attempts and other common attacks, report attacks and suspicious activity, comply with acceptable use policies, and perform basic cyber hygiene tasks (e.g., patching software, choosing passwords, protecting credentials)
    - Explain the consequences of cybersecurity policy violations, both to individual users and the organization.

- Assess or test, periodically, users on their understanding of basic cybersecurity practices. This requires annual refreshers to reinforce existing practices and introduce new practices.

- **PR.AT-2:** Privileged users understand roles & responsibilities
- **State Min Requirement:** 1
- **Best Practices:**
  - Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, finance personnel, senior leadership, and anyone with access to business-critical data.
  - Provide role-based cybersecurity awareness and training to all those in specialized roles, including contractors, partners, suppliers, and other third parties.
  - Assess, periodically, or test users on their understanding of cybersecurity practices for their specialized roles. d) Require annual refresher to reinforce existing practices and introduce new practices.

- **PR.AT-4:** Senior executives understand roles & responsibilities
- **State Min Requirement:** 1
- **Best Practices:**
  - Ensure that the selected Tiers align with organizational goals, are feasible to implement, and effectively reduce cybersecurity risks to critical assets and resources (NIST CSF 2.0).
  - Train users on information risk management methodology and approach.
  - Share intelligence from the risk management activities (when you find that there is a threat attack NIST wants you to share that).

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **PR.AT-5:** Physical and information security personnel understand roles & responsibilities
- **State Min Requirement:** 1
- **Best Practices:**
  - Prepare an Annual Communication and Awareness Training Plan.
  - Chart a Learners Taxonomy and Verb list of accountable people.
  - Create a NIST Cybersecurity Framework (Roles and Responsibilities table which can be summarized and communicated in a chart).
  - Teach how to recognize phishing attempts, understand data protection measures, and - Promote a security-conscious culture.

- **PR.DS:** Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
  - **PR.DS-1:** Data-at-rest is protected
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources.
    - Use full disk encryption to protect data stored on user endpoints. - confirm the integrity of software by validating signatures.
    - Restrict the use of removable media to prevent data exfiltration.
    - Secure, physically, removable media containing unencrypted sensitive information, such as within locked offices or filing cabinets.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **PR.DS-2:** Data-in-transit is protected
- **State Min Requirement:** 1
- **Best Practices:**
  - Initiate requests for new access or additional access for employees, contractors, and others, and track, review, and fulfill the requests, with permission from system or data owners when needed.
  - Issue, manage, and revoke cryptographic certificates and identity tokens, cryptographic keys (i.e., key management), and other credentials.

- **PR.DS-3:** Assets are formally managed throughout removal, transfers, and disposition
- **State Min Requirement:** 1
- **Best Practices:**
  - Ensure that data stored (data-at rest) remains confidential, integral, and available. Encryption, access controls, and secure storage play crucial roles.
  - Protect data during transmission. Encryption, secure protocols, and network security measures are essential (data-in-Transit).
  - Safeguard data while it's actively processed or accessed. Access controls, encryption, and monitoring are vital (data-in-use).

- **PR.DS-5:** Protections against data leaks are implemented
- **State Min Requirement:** 1
- **Best Practices:**
  - Review logical and physical access privileges periodically and whenever someone changes roles or leaves the organization, and promptly rescind privileges that are no longer needed.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Take attributes of the requester and the requested resource into account for authorization decisions (e.g., geolocation, day/time, requester endpoint's cyber health).
- Restrict access and privileges to the minimum necessary (e.g., zero trust architecture).
- Review, periodically, the privileges associated with critical business functions to confirm proper separation of duties.

- **PR.IP:** Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.
  - **PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Develop, document, and disseminate a configuration management policy that covers purpose, scope, roles, responsibilities, management commitment, coordination, and compliance.

  - **PR.IP-4:** Backups of information are conducted, maintained, and tested periodically
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Conduct Regular Backups: both user-level information and system-level information.
    - Test Backups regularly to ensure their integrity and effectiveness.
    - Maintain and manage the backups consistently.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Test the contingency plan for the system at an organization-defined frequency.
- Conduct various tests to evaluate the effectiveness of the plan and readiness for execution.
- Ensure that the alternate storage site provides controls equivalent to those of the primary site.
- Exercise and test business continuity and operational resilience plans at least annually or upon significant changes.
- Backup Data Stored in the Cloud (Related Control) and verify restoration; and ensure the confidentiality, integrity, and availability of the backup, and verify data restoration for resiliency.

- **PR.IP-6:** Data is destroyed according to policy
- **State Min Requirement:** 1
- **Best Practices:**
  - Establish, document, approve, communicate, apply, evaluate, and maintain policies and procedures for the secure disposal of equipment used outside the organization's premises.
  - Create a data destruction procedure must render recovery of information impossible, if the equipment is not physically destroyed.
  - Review and update Regularly these policies and procedures.
  - Sanitize system media (both digital and non-digital) containing sensitive information before disposal or release for reuse.
  - Use organization-defined sanitization techniques and procedures.
  - Dispose of data, documentation, tools, or system components using organization-defined techniques and methods Component Disposal (SR-12). - Secure Disposal (DSP-01): Apply industry-accepted methods for secure data disposal from storage media to prevent forensic recovery1. - Key Destruction

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

(CEK-14): Define, implement, and evaluate processes, procedures, and technical measures to destroy keys stored outside a secure environment.

- **PR.IP-9:** Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed
- **State Min Requirement:** 2
- **Best Practices:**
  - Develop, document, and disseminate a contingency planning policy.
  - Define purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
  - Be consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines.
  - Implement procedures to facilitate the policy's implementation.
  - Create a contingency plan.
  - Establish an alternate processing site with necessary agreements to permit the transfer and resumption of system operations for essential functions within a defined time period consistent with recovery objectives.
  - Ensure availability of equipment and resources at the alternate site1.
  - Provide for the recovery and reconstitution of the system to a known state within a specified time period after a disruption, compromise, or failure.

- **PR.IP-10:** Response and recovery plans are tested
- **State Min Requirement:** 2
- **Best Practices:**

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Regularly test your contingency plans for the system. The frequency of testing should be determined by your organization.
- Use various tests to evaluate the effectiveness of the plan and readiness to execute it. These tests can include tabletop exercises, simulations, and comprehensive drills.
- Review the test results and initiate corrective actions if necessary.
- Test Incident Response Capabilities (Control IR-3).
- Ensure that your incident response plan is robust and can effectively handle security incidents.
- Implement Testing, Training, and Monitoring (Control PM-14).
- Review testing, training, and monitoring activities to align them with your risk management strategy and organization-wide priorities.
- Test your organizational incident response capabilities to identify weaknesses or deficiencies.
- Use checklists, walk-through exercises, simulations, and comprehensive drills to assess your incident response readiness.
- Establish, document, and communicate a disaster response plan to recover from natural and man-made disasters.

- **PR.IP-11:** Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).
- **State Min Requirement:** 1
- **Best Practices:**
  - Integrate cybersecurity risk management considerations into human resources processes (e.g., personnel screening, onboarding, change notification, offboarding)
  - Consider cybersecurity knowledge to be a positive factor in hiring, training, and retention decisions.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

        - Conduct background checks before onboarding new personnel for sensitive roles and periodically repeat them.
        - Define and enforce obligations for personnel to be aware of, adhere to, and uphold security policies as they relate to their roles.

    - **PR.IP-12:** A vulnerability management plan is developed and implemented
    - **State Min Requirement:** 2
    - **Best Practices:**
        - Use vulnerability management technologies to identify unpatched and misconfigured software
        - Assess network and system architectures for design and implementation weaknesses that affect cybersecurity
        - Review, analyze, or test organization-developed software to identify design, coding, and default configuration vulnerabilities.
        - Assess facilities that house critical computing assets for physical vulnerabilities and resilience issues.
        - Monitor sources of cyber threat intelligence for information on new vulnerabilities in products and services.
        - Review processes and procedures for weaknesses that could be exploited to affect cybersecurity.

- **PR.MA:** Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedure
    - **PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools
    - **State Min Requirement:** 1
    - **Best Practices:**

- Integrate cybersecurity considerations throughout the life cycles of systems, hardware, software, and services
- Integrate cybersecurity considerations into product life cycles
- Identify unofficial uses of technology to meet mission objectives (i.e., shadow IT).
- Periodically identify redundant systems, hardware, software, and services that unnecessarily increase the organization's attack surface.
- Properly configure and secure systems, hardware, software, and services prior to their deployment in production.
- Update inventories when systems, hardware, software, and services are moved or transferred within the organization.
- Securely destroy stored data based on the organization's data retention policy using the prescribed destruction method and keep and manage a record of the destruction.
- Securely sanitize data storage when hardware is being retired, decommissioned, reassigned, or sent for repairs or replacement.
- Offer methods for destroying paper, storage media, and other physical forms of data storage.

- **PR.MA-2:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
- **State Min Requirement:** 1
- **Best Practices:**
  - Perform routine and emergency patching within the timeframes specified in the vulnerability management plan.
  - Update container images and deploy new container instances to replace rather than update existing instances.
  - Replace end-of-life software and service versions with supported, maintained versions.
  - Uninstall and remove unauthorized software and services that pose undue risks.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Uninstall and remove any unnecessary software components (e.g., operating system utilities) that attackers might misuse.
- Define and implement plans for software and service end-of-life maintenance support and obsolescence.

- **PR.PT:** Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.
  - **PR.PT-1:** Removable media is protected, and its use restricted according to policy
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Configure all operating systems, applications, and services (including cloud-based services) to generate log records.
    - Configure log generators to securely share their logs with the organization's logging infrastructure systems and services.
    - Configure log generators to record the data needed by zero-trust architectures.

  - **PR.PT-2:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of stored data in files, databases, virtual machine disk images, container images, and other resources.
    - Use full disk encryption to protect data stored on user endpoints
    - Confirm the integrity of software by validating signatures.
    - Restrict the use of removable media to prevent data exfiltration.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Secure, physically, removable media containing unencrypted sensitive information, such as within locked offices or filing cabinets.

- **PR.PT-3:** Removable media is protected, and its use restricted according to policy
- **State Min Requirement:** 1
- **Best Practices:**
  - Establish, test, deploy, and maintain hardened baselines that enforce the organization's cybersecurity policies and provide only essential capabilities (i.e., principle of least functionality).
  - Review all default configuration settings that may potentially impact cybersecurity when installing or upgrading software.
  - Monitor implemented software for deviations from approved baselines.

- **PR.PT-4:** Communications and control networks are protected
- **State Min Requirement:** 1
- **Best Practices:**
  - Segment organization networks and cloud-based platforms according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and permit required communications only between segments.
  - Segment organization networks from external networks and permit only necessary communications to enter the organization's networks from the external networks.
  - Implement zero trust architectures to restrict network access to each resource to the minimum necessary.
  - Check the cyber health of endpoints before allowing them to access and use production resources.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

6.3 Detect (DE) Controls

Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.

- **DE.AE - Anomalies and Events:** Anomalous activity is detected, and the potential impact of events is understood.
  - **DE.AE-2:** Detected events are analyzed to understand attack targets and methods
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Utilize security information and event management (SIEM) tools to continuously monitor logs
    - Manually review log events for anomalies, false negatives, etc.
    - Establish a scale for classifying the impact of an incident by severity (low, medium, and high).

  - **DE.AE-3:** Event data are aggregated and correlated from multiple sources and sensors
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Maintain multiple types of logs that can assist with security and access audits
    - Receive log files from API activity, domain error logs, and service error logs
    - Maintaining accurate logs and reviewing them regularly can help diagnose availability issues.

  - **DE.AE-4:** Impact of events is determined
  - **State Min Requirement:** 1
  - **Best Practices:**

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

        - Configure SIEM tools to determine and highlight the severity and impact of threats
        - By utilizing threat intelligence feeds, one could monitor and detect events like malicious IPs and unauthorized, unexpected activity

    - **DE.AE-5:** Incident alert thresholds are established
    - **State Min Requirement:** 1
    - **Best Practices:**
        - Establish an incident handling process that aligns with the incident response plan
        - Coordinate activities with contingency planning activities
        - Review and update policies and procedures at least annually
        - Ensure that all stakeholders are aware and alert of their responsibilities

- **DE.CM - Security Continuous Monitoring:** The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures
    - **DE.CM-1:** The network is monitored to detect potential cybersecurity events
    - **State Min Requirement:** 1
    - **Best Practices:**
        - Utilize software that logs user details like who and how they logged in
        - Develop and implement a continuous monitoring strategy that coordinates with the organization-level CM strategy
        - Configure firewalls to filter known malicious activity and recognize denial-of service events

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **DE.CM-2:** The physical environment is monitored to detect potential cybersecurity events
- **State Min Requirement:** 1
- **Best Practices:**
  - Monitor logs from physical control systems to identify any unusual patterns
  - Monitor physical access controls (latches, locks, sensors) for signs of tampering
  - Implement alarm systems, security guards, cameras, etc., to monitor the physical environment

- **DE.CM-3:** Personnel activity is monitored to detect potential cybersecurity events
- **State Min Requirement:** 1
- **Best Practices:**
  - Monitor logs to find unusual access patterns and failed access attempts
  - Determine and document the types of changes to the system that are configuration-controlled
  - Document configuration change decisions associated with the system

- **DE.CM-4:** Malicious code is detected
- **State Min Requirement:** 1
- **Best Practices:**
  - Monitor wired and wireless connections from unauthorized endpoints
  - Implement a signature based, non signature based malicious code protection mechanism at system entry and exit point to detect and eradicate malicious code
  - Employ spam protection mechanisms at system entry and exit points to detect and act on unsolicited messages

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **DE.CM-7:** Monitoring for unauthorized personnel, connections, devices, and software is performed
- **State Min Requirement:** 1
- **Best Practices:**
  - Establish organization defined metrics to be monitored
  - Continuously monitor security status of organization-defined metrics
  - Perform security control assessments in accordance with the organizational CM strategy

- **DE.CM-8:** Vulnerability scans are performed
- **State Min Requirement:** 1
- **Best Practices:**
  - Organization determines the required vulnerability scanning for all security components, ensuring to include networked printers, scanners, and copiers
  - Determine a testing strategy and criteria for acceptance of systems, upgrades and new versions. Automate when applicable and possible
  - Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis

- **DE.DP - Detection Process:**

  DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability

  State Min Requirement: 1

  Best Practices:
  - Define, implement, and evaluate processes, procedures and defense-in-depth techniques for protection, detection, and timely response to network-based attacks

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- Establish and maintain an incident response process that addresses roles and responsibilities, compliance requirements, and a communication plan
- Designate one key person, and at least one backup, who will manage the enterprise's incident handling process

- **DE.DP-2:** Detection activities comply with all applicable requirements
- **State Min Requirements:** 1
- **Best Practices:**
  - Implement a process for ensuring that organizational plans for conducting security and privacy testing, training, and monitoring activities associated with organizational systems are developed and maintained, continuously executed and reviewed
  - System monitoring includes external and internal monitoring that detects unauthorized use of organizational systems

- **DE.DP-4:** Event detection information is communicated to appropriate parties
- **State Min Requirements:** 1
- **Best Practices:**
  - Select the appropriate assessor or assessment team for the type of assessment to be conducted
  - Assign key roles and responsibilities for incident response, including staff from legal, IT, information security, facilities, public relations, etc.
  - Workforce personnel and external business relationships shall consent and/or contractually agree to report all information security events in a timely manner

- **DE.DP-5:** Detection processes are continuously improved
- **State Min Requirement:** 1
- **Best Practices:**
  - Test the overall strength of an organization's defense by stimulating the objectives and actions of an attacker

6.4 Respond (RS) Controls

Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.

- **RS.RP-Response Planning:**
  - **RS.RP-1:** Response plan is executed during or after an event
  - **State Min Requirement:** 2
  - **Best Practices:**
    - Maintain and regularly review documents and procedures for identified threats and vulnerabilities

- **RS.CO -Communications:**
  - **RS.CO-1:** Personnel know their roles and order of operations when a response is needed
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Ensure that all incident response stakeholders are aware and have accepted their roles and responsibilities
    - Go through stimulation and get consent from stakeholders to ensure process is documented properly

- **RS.CO-2:** Incidents are reported consistent with established criteria
- **State Min Requirement:** 1
- **Best Practices:**
  - Have and established procedure to notify the respective parties of breaches
  - Notify law enforcement based on criteria in the incident response plan and management approval

- **RS.CO-4:** Coordination with stakeholders occurs consistently with response plans
- **State Min Requirement:** 1
- **Best Practices:**
  - Notify business partners and customers of incidents in accordance with contractual requirements

- **RS.AN- Analysis:**
  - **RS.RN-1:** Notifications from detection systems are investigated
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Utilize SIEM tools to escalate security notifications based on established thresholds
    - Analysis are manually performed to determine the severity and next steps of events identified

  - **RS.RN-2:** The impact of the incident is understood
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Security threshold is established and understood by all parties
    - A severity scale is communicated to all incident responders to determine the urgency and actions needed behind a triggered event

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

- **RS.RN-3:** Forensics are performed
- **State Min Requirement:** 1
- **Best Practices:**
  - Analysis are performed to determine what was taken place during the incident and the root cause of the incident
  - Determine the sequences of events that occurred during the incident

- **RS.RN-4:** Incidents are categorized consistent with response plans
- **State Min Requirement:** 1
- **Best Practices:**
  - Develop an incident response plan that follows the mission of the organization and provides a roadmap for implementing its incident response capability
  - Establish and maintain security incident thresholds, including at a minimum, differentiating between an incident and an event

- **RS.RN-5:** Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
- **State Min Requirement:** 1
- **Best Practices:**
  - Implement a process to ensure that plans of action and milestones for the information security, privacy, and supply chain risk management programs and associated organizational systems
  - Respond to findings from security and privacy assessments, monitoring, and audits in accordance with organizational risk tolerance

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

        - Utilize SIEM tools to receive and monitor system security alerts

- **RS.MI- Mitigation:**
    - **RS.MI-1:** Incidents are contained
    - **State Min Requirement:** 1
    - **Best Practices:**
        - Utilize cybersecurity technologies and features to perform containment actions
        - Incident responders manually select and perform containment actions

    - **RS.MI-2:** Incidents are mitigated
    - **State Min Requirement:** 1
    - **Best Practices:**
        - Utilize cybersecurity technologies and features to perform incident mitigation
        - Incident responders manually perform incident mitigation

- **RS.IM- Improvements:**
    - **RS.IM-1:** Response plans incorporate lessons learned
    - **State Min Requirement:** 2
    - **Best Practices:**
        - Conduct post-incident reviews to help prevent incident recurrence through identifying lessons learned and follow-up action
        - Update incident response plans and SIEM tools based on lessons learned to prevent future events

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

6.5 Recovery (RC) Controls

Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident

- **RC.RP-1-Recovery Planning:**
  - **RC.RP-1:** Recovery plan is executed during of after a cybersecurity incident
  - **State Min Requirement:** 2
  - **Best Practices:**
    - Begin executing a recovery plan as soon as one is aware of a cyber incident
    - Ensure that all involved parties are aware of their roles and responsibilities and are present to execute

- **RC.CO-1-Communications:**
  - **RC.CO-1:** Public relations are managed
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Have a developed breach notification plan to bring awareness to the incident

  - **RC.CO-3:** Recovery activities are communicated to internal stakeholders and executive and management teams
  - **State Min Requirement:** 1
  - **Best Practices:**
    - Update regularly internal stakeholders, executives and management teams on the progress of the incident
    - Make sure to update third party vendors and suppliers about related incident

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700

7. Appendices

7.1 Appendix A Maryland Local Cybersecurity Assessment Tool

Maryland's Local Cybersecurity Assessment tool follows the NIST CSF (v1.1) framework. Each control will be scored with the maturity scale for both the National Cybersecurity Review (NCSR) and the State Minimum Cybersecurity Standards (SMCS). This will allow you to submit both the NCSR and fulfill the certification requirement for the SMCS.

Click here to access the Local Cybersecurity Assessment Tool.

You can use the tool to begin collecting the documentation needed to complete the assessment.

Recommended Steps:

1. Create a folder for the corresponding documents
2. Label each document (number and name) for easy reference in the tool
3. Write a high-level description of the corresponding document, process, or procedure in the tool.
4. If you do not have a corresponding document, process, or procedure, write: N/A. That will become part of the remediation process.

100 Community Place, Crownsville, MD 21032 | 300-301 West Preston Street, Baltimore, MD 21201
DOIT.MARYLAND.GOV - 410-697-9700