Pacific Northwest
NATIONAL LABORATORY

PNNL-36288

# Countering Weapons of Mass Destruction (CWMD) Device Cybersecurity Characterization Process and Profile

July 2024

Penny McKenzie
Mark Watson
Starr Abdelhadi
Lori Ross O'Neil
Lisa Campbell

U.S. DEPARTMENT OF ENERGY

Prepared for the U.S. Department of Energy
under Contract DE-AC05-76RL01830

## DISCLAIMER



PACIFIC NORTHWEST NATIONAL LABORATORY
*operated by*
BATTELLE
*for the*
UNITED STATES DEPARTMENT OF ENERGY
*under Contract DE-AC05-76RL01830*

**Printed in the United States of America**

**Available to DOE and DOE contractors from**
**the Office of Scientific and Technical Information,**
**P.O. Box 62, Oak Ridge, TN 37831-0062**
**www.osti.gov**
**ph: (865) 576-8401**
**fox: (865) 576-5728**
**email: reports@osti.gov**

**Available to the public from the National Technical Information Service**
**5301 Shawnee Rd., Alexandria, VA 22312**
**ph: (800) 553-NTIS (6847)**
**or (703) 605-6000**
**email: info@ntis.gov**
**Online ordering: http://www.ntis.gov**

PNNL-36288

# Countering Weapons of Mass Destruction (CWMD) Device Cybersecurity Characterization Process and Profile

July 2024

Penny McKenzie
Mark Watson
Starr Abdelhadi
Lori Ross O'Neil
Lisa Campbell

Prepared for
the U.S. Department of Energy
under Contract DE-AC05-76RL01830

Pacific Northwest National Laboratory
Richland, Washington 99354

# Summary

Countering Weapons of Mass Destruction (CWMD) recognizes that threats in the cyberspace domain continue to grow, which requires CWMD devices and supporting systems to be both cybersecure (ability to protect or defend from cyber-attacks) and resilient (ability to maintain required capability in the face of adversity) to cyber threats. The CWMD cybersecurity characterization approach in this document supports existing cyber resilience activities within the Acquisition Lifecycle Framework. Similarly, this process supports existing Department of Homeland Security Cyber Resilience Test and Evaluation activities, which consist of iterative processes, starting at the initiation of system acquisition and continuing throughout the entire device and system life cycle.

Cyber resilience is the ability of an information system to continue to operate while under attack, even if in a degraded or debilitated state,[1] and to rapidly recover operational capabilities for essential functions after a successful attack.[2]

The goal of the security characterization task for CWMD is to support the development of a CBRN device-dependent profile that aligns with device network capabilities and maps to recommended security controls to create a characterization security profile impact levels. The impact levels for CWMD devices should be characterized as Low (L), Moderate (M), High (H) to align with the low, moderate, high control baselines. To estimate the impact levels, the device's security-related attributes are translated into the security objectives: Confidentiality (C), Integrity (I), and Availability (A), known as the CIA triad.

The potential impact for each device can be L, M, H, for devices that connect and transmit different types of data and may have different impact levels. National Institute of Standards and Technology Federal Information Processing Standards Publication 199 states, "the potential impact values assigned to the respective security objectives shall be the highest value from among those security categories that have been determined for each type of information resident on the information system."[3]

As CWMD is determining the cybersecurity impact levels of CBRN devices based on network connections and data transfers, the impact levels are aligned with the associated attributes of network connections and communications. For example, if the device system is connected to a wireless network and transmits different data types based on the confidentiality of the data, the highest impact value for each security objective should represent the device's CIA impact level.

This document is intended to be used by test managers, test team, and program managers.

[1] NIST SP 800-171 Rev. 2 https://doi.org/10.6028/NIST.SP.800-171r2
[2] NIST SP 800-160 Vol. 2 Rev. 1 https://doi.org/10.6028/NIST.SP.800-160v2r1
[3] FIPS 199 https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

# Acknowledgments

The Pacific Northwest National Laboratory would like to acknowledge the T&E Cyber Team of Countering Weapons of Mass Destruction for their dedication to securing the nation and their forward-leaning approach to cybersecurity throughout the secure system life cycle, of which system characterization is a key piece.

# Acronyms and Abbreviations

| | |
|---|---|
| AC | Access Control |
| ALF | Acquisition Lifecycle Framework |
| AU | Audit and Accountability |
| CBRN | Chemical, Biological, Radiological, and Nuclear |
| CMWD | Countering Weapons of Mass Destruction |
| CRBN | Chemical, Radiation, Biological, Nuclear |
| CSF | Cybersecurity Framework |
| CWMD | Countering Weapons of Mass Destruction |
| DHS | U.S. Department of Homeland Security |
| DMAMC | Data Mining, Analysis, and Modeling Cell |
| DOE | Department of Energy |
| DOS | Denial-Of-Service |
| FIPS | Federal Information Processing Standard |
| ICT | Information and Communications Technology |
| IT | information technologies |
| NICE | National Initiative for Cybersecurity Education |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Energy |
| ORD | Operational Requirements Document |
| OS | operating system |
| PM | program manager |
| PNNL | Pacific Northwest National Laboratory |
| RMF | Risk Management Framework |
| SELC | Systems Engineering Life Cycle |
| SP | Special Publication |
| SUT | Systems Under Test |
| T&E | Test and Evaluation |

# Contents



# Figures

# Tables

# 1.0 Introduction

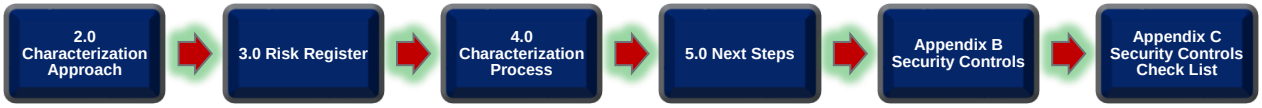


Figure 1. Document Process

## Purpose

U.S. Department of Homeland Security (DHS) Countering Weapons of Mass Destruction (CWMD) systems depend on interconnected complex environments for their systems and networks. These environments can become vulnerable. Device system assets, including their data and connections, need to be protected from security threats and vulnerabilities that could impact the CWMD mission. To protect device system assets and their information, CWMD will design, implement, and maintain a device systems security program that aligns with the DHS Cybersecurity Strategy.[1] Cybersecurity characterization of CWMD device system assets will assist in the development and fielding of more secure and resilient systems.

## Organization of the Report

This document contains seven main sections, including this introductory Section 1.0.

- Section 2.0 provides the approach to CWMD characterization processes that is essential to the support of applying the recommendations throughout the document.
- Section 3.0 identifies the risk approach.
- Section 4.0 covers Cybersecurity Impact levels and how to use them in the characterization process.
- Section 5.0 outlines the next steps identified during the characterization process.

The appendices provide additional guidance and policies that align with CWMD missions and are outlined as follows:

- Appendix A is the cybersecurity characterization definitions library that aligns with 0 controls.
- Appendix B provides the recommended cybersecurity best practices and corresponding cybersecurity controls for CWMD device systems in accordance with the Federal guidelines outlined in Appendix A.
- Appendix C provides a detailed list of U.S. Federal cybersecurity guidance to be considered before planning a characterization of Chemical, Radiation, Biological, Nuclear (CBRN) devices approach.

[1] https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf

## How to Use This Document

This document is intended to be used by test teams, test managers, and program managers to develop device and system risk characterization. It is recommended that this document be read in its entirety prior to completing the Risk Register using the five functions for framing the risk identified in Section 3.0. Once the risk has been identified using a developed risk register template, the characterization process for CBRN devices can be derived from Section 4.0 with 0 outlining the recommended best practices and corresponding security controls. Appendix C provides the CWMD cybersecurity best practices for CBRN devices, the Related NIST 800-53R5 Controls mapping, the associated risk impact levels (Low/Mod/High), and the informative references to the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Appendix C can be used by subject matter experts as a security control checklist to benchmark the implementation of security controls (Fully, Partially, or Not Implemented) and can also be referenced by program managers to document CBRN device security coverages.

### CWMD Cybersecurity CBRN Device Characterization Approach

Pacific Northwest National Laboratory (PNNL) has developed a cybersecurity device characterization process and analyzed the main policy-driven guidelines to provide CWMD with a holistic approach to cybersecurity for their CBRN devices and systems. The PNNL team reviewed all CWMD policy guidelines in 0 when developing the approach to ensure that the security applications would adhere to the needs of CWMD. The developed approach provides insight into the security-related applications needed for CBRN devices based on network connectivity, information processed and exchanged, and outside interaction with the devices. This approach is expressed in two ways:

1. Adapt existing guidelines to CWMD systems for a holistic risk-based application focused on threats to CWMD systems.
2. Integrate system network communications and connections risks to the CBRN devices.

This document provides an overview of the security best practices for CWMD CBRN systems and describes the controls that are planned for implementation or are already in place. The security controls that are appropriate align with the information that is being transmitted, processed, or stored by the system. The characterization also considers the system boundary when determining what security applications need to be in place. If the security boundary changes, then the device in question will need to be reevaluated and additional security may need to be implemented. Proper management is essential to assure that the confidentiality, integrity, and availability of the device is properly protected, and the needed security controls are applied. The implementation also includes any requirements that are set forth by applicable laws, regulations, CWMD policies, procedures, and practices.

# 2.0 Device Systems Functions and Connections

Gathering cyber characterization elements during the current Test and Evaluation (T&E) characterization process can lead to the security validation of equipment to support the acquisition process. The cyber characterization elements should be collected during testing events and integrated into data collection tools. CWMD T&E can quickly highlight and isolate information about all systems under test (SUT) that the organization has previously tested. This allows CWMD to remain agile in a changing cyber landscape as well as make informed decisions based on the identified requirements. Similar devices can be grouped together to help characterize and baseline devices in order to effectively isolate possible vulnerabilities.

At several points during a testing event and its life cycle, CWMD T&E will need to integrate cyber characteristics and information gathering into its current testing life cycle. As seen in the figure below, all five general testing categories should be impacted by cyber characterization.

- Establishing specific cyber characteristic needs and requirements
- Characterizing SUTs
- Testing SUTs based on cyber requirements
- Reporting on outcomes of cyber testing requirements
- Cataloging cyber characteristics of devices, allowing for future modeling and replay ability from information gathered using current CWMD library tools.


Figure 2. Testing Categories

Cyber Lexicons have also been developed to better categorize and recognize the cybersecurity needs of CWMD (0). As each system goes through the characterization process, the lexicons can provide the definitions for the testing that is needed to assure continued cyber resilience.

The next sections describe the actions to be taken to carry out the device and system characterization process to prepare for the CWMD T&E.

## Asset Characterization

The first step for cyber characterization of a device involves the identification of the assets in the overall system and the device connected to and interacting with. It is imperative to understand the types of assets to assure that all connection types, data, and processing are identified by CWMD. Developing an asset inventory, location identification, and connections to other functions can assure that the security characterization is applied and deployed correctly. If the inventory is missing or not complete, the characterization may be inadequate to assure the proper security controls are in place for the device.

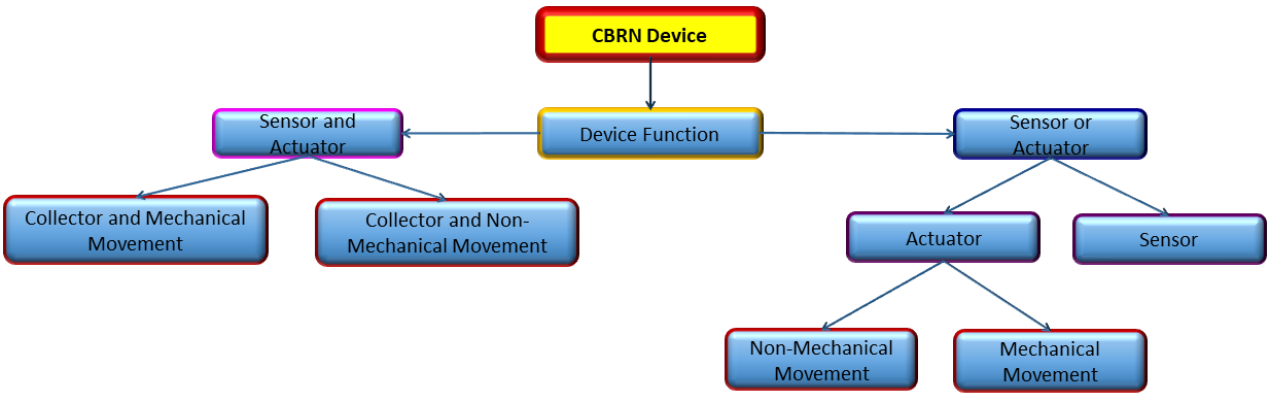


Figure 3. Generic Asset Types

## Asset Dependencies

The characterization process for CWMD CBRN devices continues by determining the information types that can be stored and processed by the device systems and the potential impact on CWMD operations, assets, individuals, or the nation should there be a loss in confidentiality, integrity, or availability. This can be done by identifying the available documentation on the devices to identify the types of information that can be processed, stored, or transmitted inside and outside of the controlling organization. Other documentation that should be included is any organizational-specific guidance and recommendation guidance from U.S. federal organizations, such as NIST, for the device in question (see 0). Also in consideration should be the system description, along with the architecture identifying where the device resides within a connected system. The characterization process may also impact other parts of the CWMD organization depending on the accuracy and categorized dependencies of the system. The figure below shows Asset Dependencies to consider while the asset inventory process is being conducted.

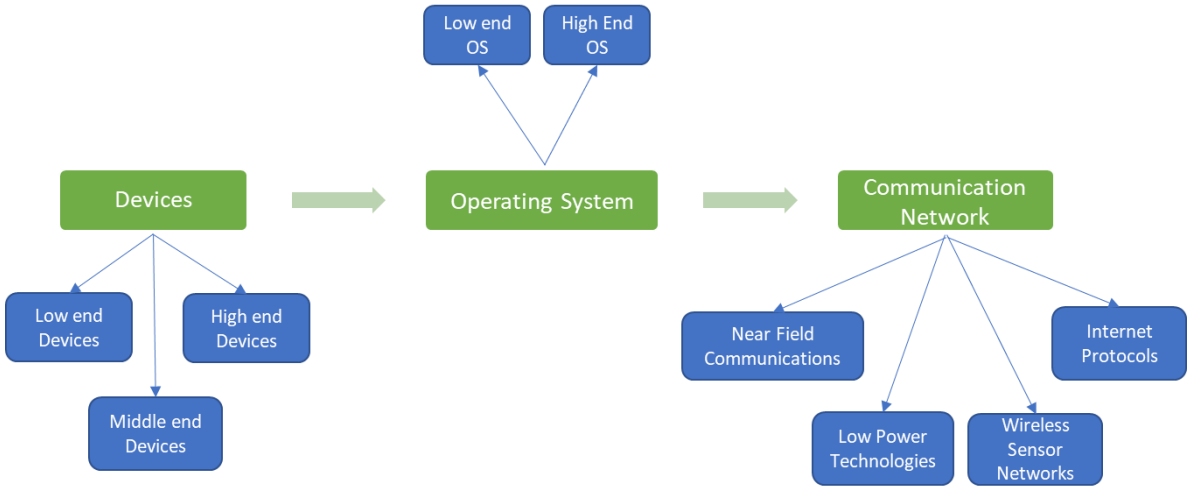


Figure 4. Asset Dependencies

## Network Characterizations

The impact could include the security program office, the architecture developers, and information sharing partners. CWMD will have to work with others that are knowledgeable about the system to determine the system boundary. Once the system boundary has been identified, CWMD will determine the low, medium, or high security controls that will be applied to the device based on that system boundary. Considerations will have to be made on the type of system connections to the overall architecture of the network connections that each system is connected to. This can include system communications (e.g., wireless, Bluetooth, Cellular (3G, 4G, 5G)) and communications protocols used by the system overall. Communication types are shown in the figure below.

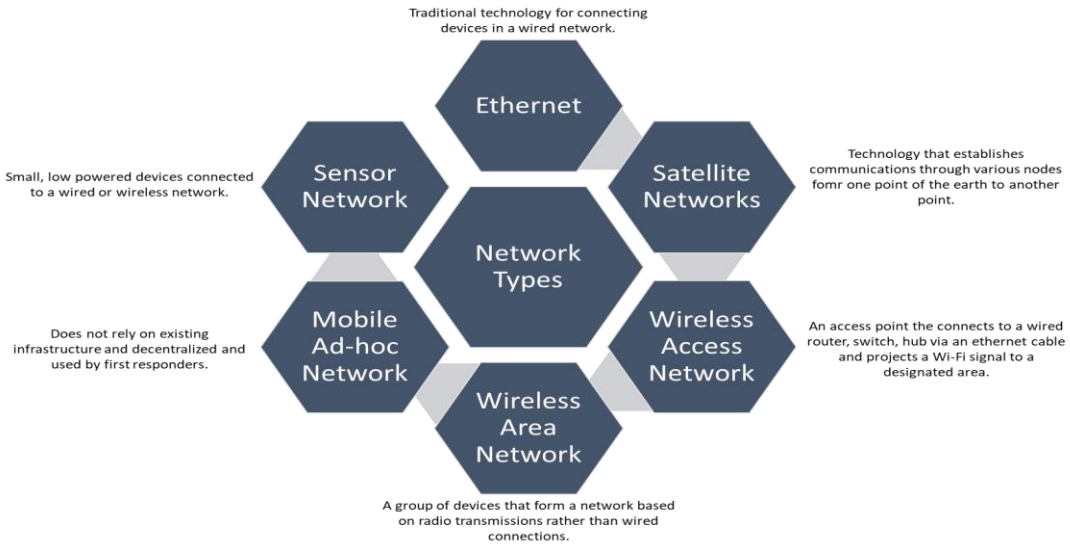


Figure 5 CWMD Network Connection Types

## Network Dependencies

There are many different connection types that can be used to manage CBRN devices and transmit data in real-time. The connection types that are used provide added flexibility to deployments and functionality for the end user. Stand-alone systems can use Wi-Fi or Bluetooth technology for short range communication and remote monitoring. Coupled with mobile devices (e.g., tablets, cell phones), gathering, managing, and transmitting data is essential to enabling real-time decisions on the health impact to personnel and the public.

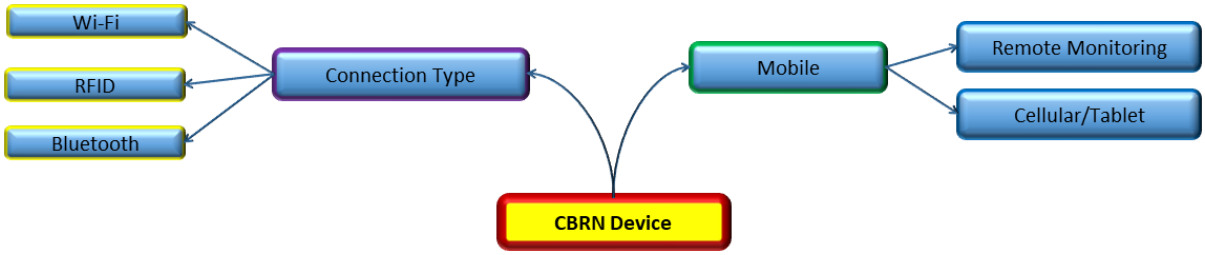


Figure 6. Generic CBRN Network Dependencies

Considerations for these types of connections should include the added security that should be applied during deployments. There are multiple dependencies that can influence the security characterization of CBRN devices. The security controls for the connection types are identified in 0 based on NIST Special Publication (SP) 800-53[1] and NIST 800-213A.[2]

[1] Security and Privacy Controls for Information Systems and Organizations https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

[2] IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog https://csrc.nist.gov/publications/detail/sp/800-213a/final

# 3.0 Risk Lifecycle

The base cybersecurity characterization implements five functions of the risk lifecycle including, framing the risk, assessing the risk, responding to the risk, monitoring the risk, and recovery and mitigation from cyber risk, threats, and vulnerabilities during the device life cycle. When considered together, these risk functions provide a high-level strategic view of the life cycle of CWMDs cyber risk management process before, during, and after the acquisition life cycle. The risk functions shown in the figure below are derived from the Cybersecurity Framework[1] (CSF) guidelines for Identify, Protect, Detect, Respond, and Recover.[2] These risk functions can aid the CWMD Test Team, test managers, and program managers to easily communicate device and system risk characterization of CBRN devices at a high level and enable risk management decisions that support mission dependencies across the systems security program. The CWMD cyber characterization processes and associated risks are described below. This is referenced in 0.


Figure 7. Risk Determination Functions

The five risk functions are key components for CWMD cyber characterization processes and should be considered when determining security controls for CBRN devices.

When considering the Risk Register, a table should be developed to document and track the security category for each system with provisional characterization types until the final characterization has been determined for the system. The risk determination helps assure that a comprehensive risk identification is considered based on the network types, data types, and overall assets in accordance with CWMD deployments. Table 1 shows an example Risk Register based on NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management.[3] This approach shows both identified and mitigated risks. Risk level abbreviations are L=Likelihood, I=Impact, R=Residual Risk and H=High, M=Moderate, L=Low, VL=Very Low where risk ratings come from NIST FIPS 199.

[1] NIST Cybersecurity Framework https://www.nist.gov/cyberframework/framework
[2] https://www.nist.gov/cyberframework/online-learning/five-functions
[3] NISTIR 8286 Integrating Cybersecurity and Enterprise Risk Management https://csrc.nist.gov/publications/detail/nistir/8286/final

Table 1. Example Risk Register

| Risk ID | Risk Element | Risk Event | Mitigation Approach | Risk Response | Mitigated Risk | | |
|---|---|---|---|---|---|---|---|
| | | | | | L | I | R |
| *1-1* | *Reliability of Systems* | *If data backup systems fail, there may be no backup copies of instrument or user data.* | *Mitigate* | *Backup systems are managed according to best practices. Data recovery capabilities are tested regularly.* | *VL* | *L* | *VL* |

Documentation should be reviewed and updated on a regular basis (annually) and a rationale should be given for each determination of the security category chosen for the system. Also included should be the rationale for a change in the characterization based on the needs of CWMD. A more comprehensive list of recommended security controls can be found in 0 (pg. 1).

The rest of this report section describes the strategies and functions that feed into the development, maintenance, and project management to track and work on the identified risks.

## Framing the Risk

The goal of framing the risk function is to identify cyber risks and vulnerabilities and to enable the development of managed cybersecurity risks for systems, assets, data, and capabilities. The objective is to identify and inventory all of the CWMD CBRN devices. Examples can be defined as operational technologies, information technologies, and the internet of things that are connected to CWMD device systems and aligned with the CWMD mission.

- Information Technology - *Any information technology, equipment, or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information*.[1]
- Operational Technology - *Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events.*[2,3]
- Internet of Things - *Any object or device that sends and receives data automatically through a network and can be connected to the internet.*[4]

All information provided in Section 3.0 is derived from the NIST Cybersecurity Framework and NIST 800-53r5 with recommended changes to align with the CWMD CBRN device risk application in the context of the risk lifecycle.

## Assessing the Risks

The assessing risk function is used to determine the impacts that a cybersecurity incident will have on device systems, assets, data, and networks used by CWMD. Special considerations should be taken to assure that any impacts on the CWMD mission are contained or limited to

[1] https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#I
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf
[3] https://niccs.cisa.gov/about-niccs/cybersecurity-glossary#I
[4] https://www.cisa.gov/uscert/ncas/tips/ST17-001

safeguarding continued operations. This function will also provide essential information that can inform risk-based decisions for mitigation strategies and the implementation of security controls and plans. Table 2 shows the basic recommendations for assessing the risks.

Table 2. Assessment Recommendations

| Risk Management Strategy | Develop CWMD priorities, risk tolerances, and constraints |
|---|---|
| Risk Assessment | Understand the cyber risks in all operations, individuals, and assets in CWMD. |
| Governance | Manage and monitor CWMD operational, environmental, regulatory, risk, and legal requirements. |
| Business Environment | The definition of CWMD's mission, objectives, stakeholders, and activities. |
| Asset Management | The identification of facilities, systems, services, data, and personnel used to accomplish CWMD purposes. |

## Monitoring the Risks

Monitoring the risk is a process that tracks and evaluates the levels of risk to CWMD. This can include activities that will monitor the risk management strategies of CWMD that can inform the creation of additional risk management strategies and update any outdated strategies that are no longer effective. Additional monitoring activities for cyber risks can include but are not limited to: gathering data, identifying what is vulnerable or needs patching, and monitoring information sources for breached information. The table below shows basic recommendations for monitoring risks.

Table 3. Monitoring Recommendations

| Protective Technology | Technical solutions for security and the implementation, review, documentation of log and audit records |
|---|---|
| Maintenance | Maintenance that is appropriately scheduled and implemented |
| Information protection processes and procedures | Security policies are maintained and leveraged |
| Data security | Support integrity and confidentiality of data while also making it available |
| Awareness and training | Security education |
| Identity and Access Management | Appropriate management of credentials and identities related to system users |
| Detection processes | Definition of roles and responsibilities involved in the detection and maintenance of activities detecting anomalous events and protection against cyber risks. Comply with requirements, test and improve. |
| Security continuous monitoring | Vulnerability scans monitor assets and information technology systems to identify issues in security and measure the ability of safeguards in place |

| Protective Technology | Technical solutions for security and the implementation, review, documentation of log and audit records |
|---|---|
| Anomalies and events | Detect events that are considered anomalous and understand the potential effects of these events |

## Responding to Risks

The goal of the responding to risk function is to enable CWMD to quickly respond to a cybersecurity incident to minimize the impact on CWMD device systems, assets, networks, and stakeholders. The intent is to limit the impact on other systems and minimize the duration of an event. This can include, but is not limited to, containment, auditing, eradication, and logging the incident for future lessons learned. It is important to note that a Security Response Plan should also be developed that will assure the continued mission of CWMD device systems and assets during a time of limited operations until the incident has been identified and contained. The table below shows basic recommendations for responding to risks.

Table 4. Response Recommendations

| Response planning | If a cyber incident is discovered, execute the response procedures |
|---|---|
| Communications | Notification of stakeholders through appropriate channels |
| Analysis | Investigation and examination of the detected event-the ability of the organization to act |
| Mitigation | Actions to take to prevent the cyberattack from continuing and spreading. Mitigating the potential impact of the threat |
| Improvements | Lessons learned from previous events |

## Recovery and Mitigation

The recovery and mitigation functions should provide steps for CWMD to restore device systems and the networks to a pre-incident state. The table below shows the basic recommendations for recovery and mitigation of risk.

Table 5. Recovery and Mitigation Recommendations

| Recovery planning | Recovery plans should be carried out, and in a timely manner, all affected systems should be supported, restored, and addressed |
|---|---|
| Improvements | Lessons observed during and after the incident to improve security strategies |
| Communications | Coordination efforts with all involved |
| Integrity | Check the system integrity before redeployments |
| Security levels | Determine the security level that should either be updated or reapplied to the device systems |
| Security testing | Test of the device systems to assure that containment has occurred, and the incident has been eradicated. |

# 4.0 Cybersecurity Characterization Process

Once CWMD has identified the CBRN devices and network types, initial impact values can be assigned to the system in question. The impact levels are based on a security scale of low, moderate, and high for the security objectives of confidentiality, integrity, and availability.[1] Each impact level aligns with the risks that could occur if the CBRN device functions are degraded or compromised, leading to additional risks to the environment, the individual, or a population. The defined controls in 0 align with NIST-SP 800-53R5 and NIST-SP 800-213A, and the impact levels can be aligned with each recommended control and best practices.

Low Impact: *The loss of confidentiality, integrity, or availability that could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States (i.e., 1) causes a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; 2) results in minor damage to organizational assets; 3) results in minor financial loss; or 4) results in minor harm to individuals).*

Moderate Impact: *The loss of confidentiality, integrity, or availability that could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States (i.e., 1) causes a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in significant damage to organizational assets; 3) results in significant financial loss; or 4) results in significant harm to individuals that does not involve loss of life or serious life-threatening injuries).*

High Impact: *The loss of confidentiality, integrity, or availability that could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States; (i.e., 1) causes a severe degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; 2) results in major damage to organizational assets; 3) results in major financial loss; or 4) results in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries).*

Confidentiality: *Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.*

Availability: *Ensuring timely and reliable access to and use of information*.

Integrity: *Guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.*

[1] https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf

## Overview of Security Controls and Characterization Process for CBRN Devices

The device characterization best practices outlined in Appendix B identify security controls that align with NIST 800-53 and NIST SP 800-213A. Each control has exclusive properties that provide the necessary guidance and best practices for the security applications of CBRN devices. Once the security control has been identified, the best practices are provided for added context on the configurations needed to comply with the security characterization of a CBRN device. In addition to Appendix B, a spreadsheet may be converted into a tabular format (e.g., .csv, .xlsx, etc.) to provide the security alignments with the best practice documentation outlined in Appendix C, the FIPS 199 security impact levels, and the NIST informative references. The NIST informative references include NIST 800-53 R5 security controls and the corresponding Cybersecurity Framework categories and sub-categories. Appendix C can be used to identify which controls have been implemented on CBRN devices in their operating environment across three categories (e.g., fully implemented, partially implemented, and not implemented).

It is not expected that each control or risk will perfectly align with all CBRN device needs and deployments, but rather provide guidance on what may be missing for device configurations, identify shortfalls in CBRN device development, and what can be addressed during a test event.

# 5.0 Next Steps

This report documents how to identify assets to test as well as how to carry out a characterization process. The process described in this report lays a solid foundation for safe and secure CWMD device systems. Additional security to be carried out include:

- Develop a more comprehensive NIST security control overlay with respect to the CWMD CBRN devices.
- Perform the actual testing based on the process described in this document and documenting outcomes and a plan of action to address any identified weaknesses, such as remediation or new device systems.
- Develop operating procedures for CWMD personnel to carry out the cyber characterization T&E process.
- Develop and train CWMD T&E personnel on the cyber characterization T&E process.
- Complete a Risk Register specific to the special needs of CWMD and complete and maintain the developed Risk Register.
- Identify how the outcome of the characterization process can be reused for other areas of CWMD.
- Compilation of risk identification for maturing documentation and testing of device systems.
- Identify the impact on future testing and procurement for the purpose of reducing effort and redundancy in the future.
- Identify the baseline risk levels for the Core Recommended Security Controls (0) specific to the special needs of CWMD.

# Appendix A – Cyber Definitions and Lexicons

Cybersecurity definitions excerpted from National Initiative for Cybersecurity Careers and Studies https://niccs.cisa.gov/about-niccs/cybersecurity-glossary

Table A.1. Cybersecurity Definitions

| Term | Definition |
|---|---|
| Active detection | Your organization should also actively seek to detect incidents (i.e., by manually reviewing audit logs and gathering intelligence from outside the organization). Measures should be put in place to help detect malicious activity that might otherwise be difficult to identify. |
| Asset management | Assets (both information and physical) should be logged, tracked, and managed throughout their life cycle. Each asset should have a defined 'owner' who is responsible for it. |
| Continual improvement process | A process to continually review and improve the organization's security measures, and to adapt to the changing threat landscape. This might include adopting well-known improvement models such as PDCA (Plan-Do-Check-Act). |
| Continuity management | Measures for identifying the risk of exposure to internal and external threats, and for dealing with major disruptions like cyber-attacks, floods, and supply failures. |
| Encryption | Your organization should have a documented process that defines when and how encryption is applied to protect information, taking account of information both in transit and at rest. |
| External validation/certification | Certification to international standards or established cybersecurity frameworks provides external validation of your organization's cybersecurity and resilience and can provide assurance to customers and other stakeholders. In some cases, third parties may require compliance audits or validation through a specific scheme. |
| Formal information security management program | There should be a structured approach to securing information assets across your organization, taking account of people, processes, and technology. This approach should unify the other processes. |
| Governance structure and processes | The organization has clear governance structures and defined lines of responsibility and accountability to oversee its cybersecurity and resilience processes. This might include organizing different elements of the framework into functions overseen by an accountable director or governance committee. |
| Information and Communications Technology (ICT) continuity | Plans, defined roles, training, communications, and management oversight are required for quickly discovering an incident and effectively containing the damage, eradicating the threat, and restoring the integrity of affected network and systems. There are agreed thresholds and timescales for recovering ICT functions following an incident. |
| Identity and access control | Measures should be implemented to assure that people attempting to access information and information systems are who they say they are and that they are authorized to access that information. This needs to include physical access as well as logical access. |
| Incident response management | ICT services are resilient in the event of disaster and can be recovered within timescales agreed with senior management. |

| Term | Definition |
|---|---|
| Information and security policies | You should document how your organization plans to protect its physical and information assets. Policies should be communicated to, and understood by, all staff and contractors. |
| Information sharing and collaboration | Threat and vulnerability information is shared among suppliers, partners, industry bodies, and authorities to enhance the collective ability to proactively detect, prevent, mitigate, respond to, and recover from cybersecurity incidents. |
| Internal audit | A program of regular audits assesses the organization's information security controls. The results are assessed as part of a senior management review. |
| Leadership-level commitment and involvement | The leadership endorses, supports, and participates in the cybersecurity strategy, and receives regular updates on security issues, risks, and compliance. |
| Malware protection | Software and other technical measures should protect your computer systems and information from a broad range of malware (including computer viruses, worms, spyware, botnet software, and ransomware). |
| Network and communications security | Your organization's network infrastructure should be secured with appropriate technologies and processes, such as switches, firewalls, segregation, and demilitarized zones. This might include securing physical communications assets such as cabling. |
| Patch management | Your organization should have a process defining how software on computers and network devices is kept up to date. Patch management processes might also affect procurement policies to assure that software is supported and will continue to receive any necessary patches, as well as to retire software that is no longer supported. |
| Physical and environmental security | Physical and environmental security controls should be implemented to reduce the risk posed by threats within the physical environment, including natural or environmental hazards, and physical intrusion by unauthorized individuals. |
| Security monitoring | Your organization's systems, networks, and security measures should be continually observed and logged, both through automated means and through less frequent activities such as vulnerability scanning and penetration testing. Any identified anomalies and weaknesses should be acted upon. |
| Security team competence and training | Security teams should be suitably qualified and regularly trained on how to respond to cybersecurity incidents. There should also be processes for developing security teams and identifying the necessary skills. |
| Staff awareness training | Employees should receive regular cybersecurity awareness training and be aware of security threats and procedures. This might include supplementary aids such as posters, briefings, etc. |
| Supply chain risk management | Your organization should have measures in place to secure information throughout the supply chain, such as security requirements in contracts, non-disclosure agreements, and rules for information sharing. These should cover the whole supply chain, including physical suppliers, software vendors, and cloud service providers. |
| Systems security | Systems should be designed to be secure, including both internal- and external-facing systems such as web applications and databases. |

# Appendix B – Cyber Security Best Practices and Controls Summary

All Controls outlined in this Appendix are derived from National Institute of Standards and Technology (NIST) SP 800-53[1] Revision 5 and NIST SP 800-213A IoT security controls.[2] Appendix C provides the CWMD Cybersecurity Best Practices and Controls Table for Chemical, Biological, Radiological, and Nuclear (CBRN) devices, the Related NIST 800-53R5 Controls mapping, the FIPS 199 security impact levels (Low/Mod/High), and the NIST informative references corresponding to the Cybersecurity Framework categories and sub-categories. Appendix C can be used by subject matter experts as a security control checklist to identify and benchmark which controls have been implemented on CBRN devices in their operating environment across three categories (e.g., Fully, Partially, or Not Implemented); assessing implementations and establishing benchmarks can also be referenced by program managers to document CBRN device security coverages. All Controls outlined in Appendix C are derived from NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations and NIST SP 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog security controls.

**Cyber Security Best Practices and Controls Summary**

**Best Practices and Controls Section Sample**

**Section Sample**
**0 Capability Name:** *Capability Text (Italicized).*
**Related CSF Category Unique Identifier:** (Function. Category)
**1.1 Sub-Capability Name** (Best Practice Identifier): Sub-Capability Text.
**Related NIST 800-213A Identifier:** Sub-Capability (requirements)

***Best Practices that may be necessary/MUST have the ability to:***
**1.1.1** Best Practice Text.
**Related NIST 800-53R5 Controls:** Control ID-Control Number (Low, Moderate, and/or High)

***1*** **Device Identification:** *MUST identify CBRN devices for multiple purposes (e.g., asset management, vulnerability management, access management, data protection, and incident detection) and in multiple ways using logical identifiers and device behavior identification to meet organizational requirements.*

[1] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf

**Related CSF Category Unique Identifier:** Identify **(**ID.AM, ID.RA), Detect (DE.AE, DE.CM, DE.DP), Protect (PR.AC, PR.DS, PR.IP, PR.PT), Respond (RS.AN, RS.CO)

**1.1 Device Identifier** (DI.DI): A unique device identifier initiates the ability to identify system elements for monitoring CBRN devices and manage assets. The CBRN devices should incorporate a unique identifier that can be used to identify the device logically. This also enables a linkage to the person or processes assigned to use the device.
**Related NIST 800-213A:** IMS(3)

***Best Practices that may be necessary/MUST have the ability to:***

**1.1.1** Employ a mechanism to uniquely identify and authenticate CBRN devices before establishing a network connection (local, remotely). Related NIST 800-53R5 Controls: IA-3 (Mod/High)

**1.1.2** Select an identifier that can be assigned to the roles, services, and individuals for CBRN devices. Related NIST 800-53R5 Controls: IA-4 (Low/Mod/High)

**1.1.3** Unique device identifiers should not be reused for any service. Related NIST 800-53R5 Controls: IA-4 (Low/Mod/High)

**1.2 Device Identify Actions** (DI.DIA): The differentiation of CBRN devices can help provide assurance on the applied security controls by monitoring the device actions based on the assigned identity.
**Related NIST 800-213A:** AID(1)(2)(3)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**1.2.1** Create a list of event types to be monitored and have mechanisms in place for auditing and record retention. This is an important step to identify a root cause of a problem. Related Control: AU-2

**1.2.2** Implement an automated mechanism for tracking assets by location and responsible individuals of CBRN devices. CWMD should have the capability to rapidly respond to a compromise and breach and apply mitigations actions in a timely manner. Related Control: CM-8 (8)

**1.2.3** Enforce approved authorizations for logical access to information and system resources in accordance with applicable CWMD access control policies. Related NIST 800-53R5 Controls: AC-3 (Low/Mod/High)

**1.2.4** Invoke internal monitoring capabilities or deploy CBRN monitoring devices strategically within the system to collect appropriate CWMD-defined essential information and at ad hoc locations within the system to track specific types of transactions of interest. Related NIST 800-53R5 Controls: SI-4 (Low/Mod/High)

**1.2.5** Analyze detected events and anomalies. Related NIST 800-53R5 Controls: SI-4 (Low/Mod/High)

**1.2.6** Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the nation. Related NIST 800-53R5 Controls: SI-4 (Low/Mod/High)

**1.3 Authentication support** (DI.AS): CWMD should be able to support CBRN interfaced device authentication. Some CBRN devices may need to authenticate their identity with other systems and other systems elements.
**Related NIST 800-213A:** IMS(1)(2), AID(1)(4), DAS(1)(2), PID(1)

***Best Practices that may be necessary/MUST have the ability to:***

**1.3.1** Limit the number of CBRN device connections based on mission needs. Related NIST 800-53R5 Controls: IA-3 (Mod/High)

**1.3.2** Enable bi-directional authentication that is cryptographically based. Related NIST 800-53R5 Controls: IA-3 (Mod/High)

**1.4 Physical Identifiers** (DI.PI): CWMD should be able to apply a mechanism to identify the CBRN device on physical attributes internally or externally unique to each device.
**Related NIST 800-213A:** IMS(1)(2), AID(1)(4), DAS(1)(2), PID(1)

***Best Practices that may be necessary/MUST have the ability to:***

**1.4.1** Periodically verify physical identifiers and logical identifiers are properly incorporated under asset management control. Related NIST 800-53R5 Controls: IA-3 (Mod/High)

***2*** **Device Configuration:** *The CBRN device should have the capability to be configured through logical and/or physical interfaces to meet CWMD requirements. This supports vulnerability management, access management, data protection, and incident detection. CWMD should be able to implement protective measures to ensure the confidentiality, integrity, and availability of the configurations.*
**Related CSF Category Unique Identifier:** Detect (DE.AE, DE.CM), Protect (PR.AC, PR.DS, PR.IP, PR.PT)

**2.1 Privileged Access Configurations** (DC.PAC): The CBRN device should support the ability to apply logical access privilege settings for authorized users to ensure the integrity of CBRN access and usage. (ORGANIZATIONAL 800-213A and 800-53 users or processes acting on behalf of organizational users).
**Related NIST 800-213A:** LA: AUN(1), AUZ(1)(2)

***Best Practices that may be necessary/MUST have the ability to:***

**2.1.1** Uniquely identify and authenticate users and associate that unique identification with CBRN device processes acting on behalf of those users. Related NIST 800-53R5 Controls: IA-2 (Low/Mod/High)

**2.2 Authentication and Authorization** (DC.AA): Must have the ability to limit any changes to CBRN devices by employing system policies for authentication and authorization. Related NIST 800-53R5 Controls: AC-3, CM-5 (See Below)
**Related NIST 800-213A:** DI: AID(1), DC: PRV(1), AUT(1), INT(1), CTL(2)(4)

**2.2.1** Enforce approved authorizations for physical access to information and system resources in accordance with applicable CWMD access control policies. Related NIST 800-53R5 Controls: AC-3, CM-5 (Low/Mod/High)

**2.2.2** Define, document, approve, and enforce physical and logical access restrictions associated with changes to the CBRN device. Related NIST 800-53R5 Controls: CM-5 (Low/Mod/High)

**2.3 Interface Configuration** (DC.IC): Only authorized CWMD personnel can configure aspects of CBRN devices.
**Related NIST 800-213A:** DI: AID(1), DC: PRV(1), AUT(1), INT(1), CTL(2)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**2.3.1** Permit authorized individuals to access CBRN devices for purpose of initiating changes. Access restrictions can include:
a. Physical and logical access
b. Software libraries
c. Abstract layers
d. Change windows (times allocated by CWMD)
Related Control: CM-5 (Low/Mod/High)

**2.4 Display Restrictions** (DC.DR): The CBRN device MUST have the ability to configure content to be displayed on a device.
**Related NIST 800-213A:** DC: DSP(1)

***Best Practices that may be necessary/MUST have the ability to:***

**2.4.1** Display system use notification message or banner prior to granting access to U.S. Government CBRN systems and/or devices. Related NIST 800-53R5 Controls: AC-8 (Low/Mod/High)

**2.4.2** Display message that CBRN device usage may be monitored, recorded, and subject to audit. Related Control: AC-8 (Low/Mod/High)

**2.4.3** Prohibit unauthorized use of the CBRN device subject to criminal and civil penalties. Related NIST 800-53R5 Controls: AC-8 (Low/Mod/High)

**2.4.4** Display message that use of the device indicates consent to monitoring and recording. Related NIST 800-53R5 Controls: AC-8 (Low/Mod/High)

**2.4.5** Display message that provides information on standard lengths of time when terminating user sessions on CBRN devices, based on the needs of the mission. Related Control: AC-12(2)

**2.1 Device Configuration Control** (DC.DCC): Have all baseline configurations for CBRN devices documented, maintained, and controlled by CWMD.

**Related NIST 800-213A:** DC: CTL(1)(2)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**2.5.1** Include the security and privacy control implementations on CBRN device components that include connectivity, operational components, and communications serve as the basis for future builds, releases, or changes to the devices. Related Control: CM-2

**2.5.2** Document the baseline configurations for operational procedures, information about the system components, and network connectivity. I to identify any unnecessary or unwanted changes. Related NIST 800-53R5 Controls: CM-2 (Low/Mod/High)

**2.5.3** Determine and document the types of changes to the CBRN devices. Related NIST 800-53R5 Controls: CM-3 (Mod/High)

**2.5.4** Review proposed configuration-controlled changes to the CBRN device and approve or disapprove such changes with explicit consideration for security and privacy impact analyses. Related NIST 800-53R5 Controls: CM-3 (Mod/High)

**2.5.5** Document configuration change decisions associated with the CBRN device. Related NIST 800-53R5 Controls: CM-3 (Mod/High)

**2.5.6** Retain records of configuration-controlled changes. Related NIST 800-53R5 Controls: CM-3 (Mod/High)

**2.5.7** Monitor and review activities associated with configuration-controlled changes to the system. Related NIST 800-53R5 Controls: CM-3 (Mod/High)

**2.5.8** Establish and document configuration settings for components employed within the CBRN device that reflect the most restrictive mode consistent with operational requirements. Related NIST 800-53R5 Controls: CM-6 (Low/Mod/High)

**2.5.9** Monitor and control changes to the configuration settings in accordance with CWMD policies and procedures. Related NIST 800-53R5 Controls: CM-6 (Low/Mod/High)

***3*** **Data Protection:** *Data protection on a CBRN device supports CWMD cybersecurity needs and goals such as access management, system and organizational data protection, and incident detection. Confidentiality, availability, and integrity of data is central to cybersecurity.*
**Related CSF Category Unique Identifier:** Detect (DE.CM), Protect (PR.AC, PR.DS, PR.IP, PR.PT)

**3.1 Cryptography** (DP.C): The CBRN device MUST have the ability to employ secured mechanisms to ensure the confidentiality of data at rest and in transit, authentication for users of CBRN devices, and to ensure secured communications when in the field.
**Related NIST 800-213A:** DS: RSC(1), DP: CRY(1)(2)(3)(4)(5), KEY(1)

***Best Practices that may be necessary/MUST have the ability to:***

**3.1.1** Prevent unauthorized or unintended transfer of information from shared resources. This includes encrypted information transfers from CBRN devices. Related Control: SC-4

**3.1.2** Use cryptography solutions to protect CBRN information (e.g., data, configurations, locations, etc.) by using NSA-approved cryptography or FIPS validated cryptography. Related Control: SC-13 (Low/Mod/High)

**3.2 System and Communications Protection** (DP.SCP): CWMD should be able to demonstrate the ability to securely initiate and terminate communications between CBRN devices and supporting systems.
**Related NIST 800-213A: CS:** EIM(6)

***Best Practices that may be necessary/MUST have the ability to:***

**3.2.1** Implement subnetworks for publicly accessible system components that are physically separated from internal organizational networks and should only be connected through managed interfaces with boundary protection in accordance with CWMD security privacy architectures (e.g., firewalls, gateways, routers, encrypted tunnels, etc.). Related Control: SC-7 (Low/Mod/High)

**3.2.2** Take precautions to limit the number of external connections to CBRN devices. Related Control: SC-7(3) (Mod/High)

**3.2.3** Protect CBRN devices that have the capability to allow additional physical connections to the device (e.g., USB, ethernet). Protections should be in place that would disallow unauthorized users from physical access to the device (card reader, locks, boxes, etc.).Related Control: SC-7(14)

**3.2.4** Prohibit the direct connection of CBRN devices to external networks (e.g., virtual interface, internet). Related Control: SC-7(25)

**3.2.5** Prohibit the direct connection of CRBN device to a public network and apply configuration management of the device when commissioned. Related Control: SC-7(28)

**3.3 Secure storage** (DP.SS): Some CBRN devices may have the capability to store data during and after use in the field. MUST have the ability to enable secure device data storage for CBRN devices.
**Related NIST 800-213A:** DP: STO(1)(2)(3)(4), STX(1)(3)

***Best Practices that may be necessary/MUST have the ability to:***

**3.3.1** Ensure that there is a system backup of CBRN devices for restoration that includes security-related documentation, system-level information, and user-level information. Related Control: CP-9 (Low/Mod/High)

**3.3.2** Ensure that the implementation of cryptographic mechanisms is in place from information backed up from CBRN devices. Related Control: CP-9(8) (Mod/High)

**3.3.3** Ensure sanitization mechanisms are commensurate with security or classification of information stored before decommissioning or disposal of CBRN devices. Related Control: MP-6 (Low/Mod/High)

**3.3.4** Protect information at rest when data has been received from CBRN devices after use. Related Control: SC-28 (Mod/High)

**3.3.5** Apply cryptographic applications to ensure the confidentiality of the CBRN data and to detect any changes to the information during transmission. Related Control: SC-8(1) (Mod/High)

***4*** **Logical access to Interfaces:** *Establish requirements for authentication and identification, configuration, and display requirements to support cybersecurity needs and goals (e.g., vulnerability management, access management, data protection, incident detection). Some CBRN devices may have access interfaces that could include physical and logical components to support its management and use.*
**Related CSF Category Unique Identifier:** Identify (ID.AM), Detect (DE.CM), Protect (PR.AC, PR.DS, PR.IP, PR.PT)

**4.1 Authentication Support and Configuration** (LAI.ASC): Support authentication methods for physical and logical access to CBRN devices.
**Related NIST 800-213A:**LA: AUN(1)(4), AUZ(1)(2), ACF(1)(2)(3), IFC(1)

***Best Practices that may be necessary/MUST have the ability to:***

**4.1.1** Implement multi-factor authentication for remote commands to ensure that CBRN devices are protected against unauthorized commands. Related Control: AC-17(10)

**4.1.2** Incorporate identification and authentication requirements for the use of CBRN devices and the transfer of CBRN data to ensure accountability and traceability of users. Related Control: IA-2 (Low/Mod/High)

**4.1.3** Disable the usage of CBRN devices when they are not in use after a designated time period until the user is able to reauthenticate their credentials. Related Control: AC-2(5)

**4.1.4** Disable access and ensure the integrity of the CBRN device has not been compromised, if the security attributes of the CBRN device have changed after being configured by CWMD. Related Control: AC-3(8)

**4.1.5** Impose a limit on how many unsuccessful logins are attempted by the user. Once the limit has been reached, the CBRN device should be locked for a designated amount of time defined by organization policy. If the maximum number of unsuccessful logins have exceeded what has been defined by organization policy, the device should lock or disable until it is released by an authority designated by designated organization. Related Control: AC-7 (Low/Mod/High)

**4.1.6** Document all allowed remote access configurations and authorized connection requirements for CBRN devices. Related Control: AC-17 (Low/Mod/High)

**4.2 Role Management** (LAI.RM): Establish unique user accounts for CBRN devices in use to ensure the correct personnel can use, handle, and operate the device based on configured CWMD user information.
**Related NIST 800-213A**: LA: ROL(1)(2)(3)(4)(5)(6), IFC(4)(5), DS: EXE(2)(3)

***Best Practices that may be necessary/MUST have the ability to:***

**4.2.1** Establish an accountability mechanism that enables the monitoring of users that have control and use a CBRN device to ensure the principle of least privilege. Related Control: AC-2 (7) (Low/Mod/High)

**4.2.2** Provide an enforcement mechanism to prevent unauthorized access or changes to a CBRN device after the initial installation of the CBRN software. Related Control: AC-3(12)

**4.2.3** Enforce the least privilege for the use of CRBN devices, allowing only authorized personnel to use or make changes to the CBRN device. Related Control: AC-6 (Mod/High)

**4.2.4** Employ a mechanism to separate user functionality from the management of the CBRN device to prevent unauthorized changes. Related Control: SC-2 (Mod/High)

**4.3 Limitations on Device Usage** (LAI.LDU): Establish restrictions or limitations for how CBRN devices can be used by internal or external users.
**Related NIST 800-213A:** LA: ROL(8), LDU(1), XCN(1)(2)(3)

***Best Practices that may be necessary/MUST have the ability to:***

**4.3.1** Determine whether access authorizations assigned to a sharing partner match user restrictions and information access to the CRBN device. Related Control: AC-21 (Mod/High)

**4.4 External Connections** (LAI.EC): Identify the security best practices for external connections when CRBN devices are operating on external networks. Some CBRN devices may need external connections that could include (e.g., wireless, Bluetooth).
**Related NIST 800-213A:** DP: STX(2)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**4.4.1** Establish identification mechanisms for external connections to CBRN devices to ensure no unauthorized connections are established without proper permission or security. Related Control: AC-20 (Low/Mod/High)

**4.4.2** Enforce restrictions on information sharing based on access restrictions and security configurations for external connections. Related Control: AC-21(1)

**4.4.3** Employ cryptographic mechanisms to protect the confidentiality and integrity of transmitted information from the CBRN device. Related Control: SC-8 (Mod/High)

**4.5 Interface Control** (LAI.IC): MUST have the ability to establish security controls for any connection to and from CBRN devices.
**Related NIST 800-213A:** LA:ROL(5),IFC(1)(3)(4)(5)(6)(8)(13)(14)(15), AFC(2), DC: PRV(1), AUT(1), INT(1), CTL(2)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**4.5.1** Enforce the principle of least privilege for the use of CRBN devices on any connection outside the control of CWMD. Related Control: AC-6 (Mod/High)

**4.5.2** Document rationale for remote access to the CBRN device in the security plan. Related Control: AC-17(4) (Mod/High)

**4.5.3** Establish the configuration requirements, connection requirements, and implementation guidance for wireless capabilities with CBRN devices, in addition to the authorization of wireless access to the CRBN device, before allowing connections. Related Control: AC-18 (Low/Mod/High)

**4.5.4** Establish an authentication and encryption mechanism that aligns with CWMD policies to protect wireless access and connection with a CBRN device. AC-18(1) (Mod/High)

**4.5.5** Disable any wireless networking capabilities embedded within CRBN system components before issuance and deployment. Related Control: AC-18(3) (Mod/High)

**4.5.6** Define, document, approve, and enforce physical and logical access restrictions associated with changes to the CBRN device. Related Control: CM-5 (Low/Mod/High)

**4.5.7** Remove unused or unnecessary software and disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Related Control: CM-7 (Low/Mod/High)

***5*** **Software Update:** *Updates for CBRN devices are essential for vulnerability management. Updates can correct operational problems with the software or firmware. Support mechanisms are in place for updates that improve availability, reliability, performance, and other aspects of CBRN operations.*
**Related CSF Category Unique Identifier:** Detect (DE.CM), Protect (PR.IP, PR.PT)

**5.1 Update Capabilities** (SU.UC): Update software within the device or through its interface with proper security in place.
**Related NIST 800-213A:** SU: UPD(2), DC: CTL(1), PRV(1), AUT(1), INT(1), CTL(2)(4**)**

***Best Practices that may be necessary/MUST have the ability to:***

**5.1.1** Develop and document an audit and accountability policy that addresses the purpose of contributing to security and privacy assurance based on CWMD mission or CRBN device specific policies and procedures. Related Control: AU-1 (Low/Mod/High)

**5.1.2** Incorporate a mechanism to test, review, and identify any changes to a CBRN device, including system upgrades and modifications. This can include any changes to baseline configurations, operational procedures, configuration settings for CBRN device components, remediation of vulnerabilities, and unscheduled or unauthorized changes. Related Control: CM-3 (Mod/High)

**5.1.3** Enforce access restrictions for changes to a CBRN device that should include physical and logical access controls by defining and documenting any associated changes to the CBRN device. Related Control: CM-5 (Low/Mod/High)

**5.1.4** Prevent the installation of any software or firmware components on a CBRN device without verification that it has been recognized and approved by CWMD. Related Control: CM-14

***6*** **Cybersecurity State Awareness:** *Prevent the unauthorized or unintended transfer of information from trusted CBRN devices. Support vulnerability management, incident detection and investigation of potential compromises, and troubleshoot from a known operational state. Capture critical CBRN device information from logging and auditing, depending on the device design, use case, or other consideration.*
**Related CSF Category Unique Identifier:** Identify (ID.BE, ID.RA, ID.SC), Detect (DE.AE, DE.CM, DE.DP), Protect (PR.AC, PR.DS, PR.IP, PR.PT), Respond (RS.AN, RS.IM, RS.CO, RS.MI, RS.RP), Recover (RC.CO, RC.IM, RC.RP)

**6.1 Access to Event Information** (CSA.AEI): MUST have the ability to access CBRN device state information and the ability to collect and make data available when necessary.

**Related NIST 800-213A:**CS: AEI(2), RDL(3), LSR(2), LSR(3), DI: AID(2)

***Best Practices that may be necessary/MUST have the ability to:***

**6.1.1** Retain audit records based on established records retention policies to support post-incident investigations. Related Control: AU-11 (Low/Mod/High)

**6.1.2** Create a list of event types to be monitored, have mechanisms in place for logging and auditing, and generate and retain audit records for select CBRN devices. This is an important step to identify a root cause of a problem. Related Control: AU-12 (Low/Mod/High)

**6.1.3** Monitor unauthorized local, network, and remote connections and detect cyberattacks and indicators of potential attacks. Related Control: SI-4 (Low/Mod/High)

**6.1.4** Identify unauthorized use of the system using established techniques and methods. Related Control: SI-4 (Low/Mod/High)

**6.1.5** Analyze detected events and anomalies from external and internal monitoring within the system. Related Control: SI-4 (Low/Mod/High)

**6.1.6** Adjust the level of system monitoring activity when there is a change in risk to system operations, CBRN devices, individuals, other organizations, or the nation. Related Control: SI-4 (Low/Mod/High)

**6.2 Event Identification & Monitoring** (CSA.EIM)**:** Provide event identification and monitoring capabilities and/or support event identification and monitoring tools interfacing with CBRN devices.

**Related NIST 800-213A:** CS: EIM(1)(2)(4)(5)(6)(7)(8)(10), DC: CTL(1)(2)(4), PRV(1), AUT(1), INT(1), LA: AUN(1), AUZ(1)(2)

***Best Practices that may be necessary/MUST have the ability to:***

**6.2.1** Deploy a mechanism for monitoring open-source information for evidence of unauthorized disclosure or data leakage attributed to CBRN-related device information. Related Control: AU-13

**6.2.2** Define personnel, roles, and actions to support notification procedures whenever information disclosure is discovered. Related Control: AU-13

**6.2.3** Develop a system-level continuous monitoring strategy that includes establishing CBRN device-level metrics, frequency of occurrence for control assessment effectiveness, correlation and analysis of information generated, response actions to address the results of control assessment analysis and reporting the security and privacy status of CBRN devices to appropriate CWMD personnel. Related Control: CA-7 (Low/Mod/High)

**6.2.4** Determine, document, and retain records of the changes to CBRN devices that are under configuration control. Related Control: CM-3 (Mod/High)

**6.2.5** Consider the security and privacy implications before making decisions to approve or disapprove proposed configuration control changes. Related Control: CM-3 (Mod/High)

**6.2.6** Implement approved configuration control changes to CBRN devices and perform associated monitoring and review activities. Related Control: CM-3 (Mod/High)

**6.2.7** Provide oversight for configuration change control activities to CBRN devices, in accordance with CWMD mission assurance levels and protection conditions. Related Control: CM-3 (Mod/High)

**6.2.8** Define, document, approve, and enforce physical and logical access restrictions associated with changes to CBRN devices and the systems they support. Related Control: CM-5 (Low/Mod/High)

**6.2.9** Enforce access restrictions for CBRN devices, where applicable, using automated mechanisms and automatically generate audit records of the enforcement actions. Related Control: CM-5(1) (High)

**6.2.10** Establish, document, and implement configuration settings for CBRN devices employed within the system that reflect the most restrictive mode consistent with operational requirements. Related Control: CM-6 (Low/Mod/High)

**6.2.11** Monitor and control changes to the configuration settings of CBRN devices, in accordance with organizational policies and procedures. Related Control: CM-6 (Low/Mod/High)

**6.2.12** Uniquely identify and authenticate users and associate that unique identification with CBRN device processes acting on behalf of those users. Related Control: IA-2 (Low/Mod/High)

**6.2.13** Implement subnetworks for publicly accessible system components that are physically separated from internal organizational networks and should only be connected through managed interfaces with boundary protection in accordance with CWMD security privacy architectures (e.g., firewalls, gateways, routers, encrypted tunnels, etc.). Related Control: SC-7 (Low/Mod/High)

**6.2.14** Prohibit remote activation of collaborative computing devices and applications (e.g., cameras, microphones, etc.) except where remote activation is authorized. Collaborative devices and applications should include signals to indicate when they are activated. Related Control: SC-15 (Low/Mod/High)

**6.2.15** Prohibit the use of individual CBRN devices from possessing other sensors and/or sensing capabilities (e.g., mobile devices, cellular phones, smart phones, tablets, etc.) that are designated for CWMD-defined operating environments, facilities, or systems. Related Control: SC-42

**6.2.16** Configure CBRN devices so that only data or information collected by the CBRN sensors and/or sensing capabilities is reported to authorized individuals or roles. Related Control: SC-41(1)

**6.3 Event Response** (CSA.ER): Enable response features or functions that support event monitoring requirements.
**Related NIST 800-213A:** CS: EVR(1)(2)(3)(4)(5)(7)(8)(9)(10)(11)

***Best Practices that may be necessary/MUST have the ability to:***

**6.3.1** Provide and implement a central viewing process to analyze data (audit or data) from multiple components on the system. Related Control: AU-6(4) (Low/Mod/High)

**6.3.2** Define an alternative or supplemental security mechanism on the CBRN device when the primary means of implemented security function is unavailable or compromised. Related Control: CP-13 (Low/Mod/High)

**6.3.3** Implement an incident handling capability consistent with the incident response plan (e.g., preparation, detection and analysis, containment, eradication, and recovery). Related Control: IR-4 (Low/Mod/High)

**6.3.4** Coordinate incident handling activities with contingency planning activities. Related Control: IR-4 (Low/Mod/High)

**6.3.5** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly. Related Control: IR-4 (Low/Mod/High)

**6.3.6** Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization. Related Control: IR-4 (Low/Mod/High)

**6.3.7** Develop a risk response guide that can be used when findings from security assessments and monitoring are outside the threshold of CWMD's risk tolerance. Related Control: RA-7 Risk Response (Low/Mod/High)

**6.4 Logging Capture & Trigger Support** (CSA.LCTS): Generate, store, retain, delete, and report on specific CBRN device audit events, run specific audit checks, and report findings in a variety of ways.
**Related NIST 800-213A:** DI: AID(2), CS: LCT(1), RDL(1)(2)(5)

***Best Practices that may be necessary/MUST have the ability to:***

**6.4.1** Ensure that audit records contain information that establish the following essential elements of event information: What type of event occurred; When the event occurred; Where the event occurred; Source of the event; Outcome of the event; and Identity of any individuals, subjects, or objects/entities associated with the event. Related Control: AU-2 (Low/Mod/High)

**6.4.2** Capture audit record content that supports auditing functions, including event descriptions, time stamps, source and destination addresses, user or process identifiers, successful or failed indications, and filenames. Related Control: AU-3 (Low/Mod/High)

**6.5 Support of Required Data Logging**(CSA.SRDL): Capture required information in audit logs.
**Related NIST 800-213A**:DI: AID(2), CS: LCT(1), RDL(1)(2)(5)(7), LSR(2)(3)(4), AEI(2)

***Best Practices that may be necessary/MUST have the ability to:***

**6.5.1** Retain all CBRN device audit records consistent with the CWMD records retention policy for a (CWMD-defined time period) to support post-incident investigations that meet CWMD information retention requirements. Related Control: AU-11 (Low/Mod/High)

**6.5.2** Identify the types of events (e.g., password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage) that CBRN devices are capable of logging in support of auditing. Related Control: AU-2 (Low/Mod/High)

**6.5.3** Ensure that audit records contain information that establishes the following essential elements of event information:
a. What type of event occurred;
b. When the event occurred;
c. Where the event occurred;
d. Source of the event; Outcome of the event; and
e. Identity of any individuals, subjects, or objects/entities associated with the event.
Related Control: AU-3 (Low/Mod/High)

**6.5.4** Implement audit log retention requirements and allocate supporting audit log storage capacities for CBRN devices. Related Control: AU-4 (Low/Mod/High)

**6.5.5** Alert within a (CWMD-defined time period) when allocated audit log storage volumes reach a (CWMD-defined percentage) of maximum audit log storage capacity. Related Control: AU-5(1) (High)

**6.5.6** In the event of a primary audit logging failure, connect to an alternate audit logging capability that implements a minimum standard of auditing functionality determined by CWMD. Related Control: AU-5(5)

**6.6 Support for Reliable Time** (CSA.SRT): Use timestamps to record the time an auditing event occurred.
**Related NIST 800-213A:** CS: SRT(1)(2)(3)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**6.6.1** Generate time stamps of CBRN devices for audit records using internal system clocks. Related Control: AU-8 (Low/Mod/High)

**6.6.2** Record time stamps of CBRN devices for audit records that meet (CWMD-defined time measures) that implement local time offsets from Coordinated Universal Time (UTC). Related Control: AU-8 (Low/Mod/High)

**6.6.3** Synchronize CBRN device clocks within and between systems and components to compare internal system clocks at (CWMD-defined frequencies) with UTC. Related Control: SC-45

**6.6.4** Synchronize the internal system clocks to the UTC when the difference is greater than (CWMD-defined time period). Related Control: SC-45

**6.7 Audit Support & Protection** (CSA.ASP): Support and protect audit activities and associated data for CBRN devices.
**Related NIST 800-213A:** CS: RDL(7), AUP(1)(2)(4)(5)(6)(7), EVR(3)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**6.7.1** Review and analyze CBRN device audit records for indications and potential impacts of inappropriate or unusual activity. Related Control: AU-5(5)

**6.7.2** Implement audit record reduction and report generation capabilities that maintain original content and include modern data mining techniques to identify anomalous behavior in CBRN device audit records. Related Control: AU-6 (Low/Mod/High)

**6.7.3** Protect audit information and audit logging tools from unauthorized access, modification, and deletion. Related Control: AU-7 (Mod/High)

**6.7.4** Alert appropriate personnel upon detection of unauthorized access, modification, or deletion of audit information. Related Control: AU-9 (Low/Mod/High)

**6.8 State Awareness Support** (CSA.SAS) Differentiate between a device expected operation, from when it may be in a degraded cybersecurity state.
**Related NIST 800-213A:** AWR(1)

***Best Practices that may be necessary/MUST have the ability to:***

**6.8.1** Implement the security design principle of self-analysis in CBRN devices to assess the internal state of devices for data integrity and correct functionality in accordance with CWMD-established levels of trustworthiness. Related Control: SA-8(21)

**6.8.2** Verify the correct operation of security and privacy functions for CBRN devices in order to implement transitional states, alert appropriate personnel to failed security and privacy verification tests, and perform alternative actions (e.g., shut down device(s), restart device(s)) when anomalies are discovered. Related Control: SI-6 (High)

## *7* Device Security: *CWMD organizational requirements should be taken into consideration when determining CBRN cybersecurity at the device level, which can include technical features or functions implemented in the device's hardware and software.*

**Related CSF Category Unique Identifier:** Identify (ID.AM, ID.SC), Detect (DE.AE, DE.CM, DE.DP), Protect (PR.AC, PR.DS, PR.IP, PR.PT), Respond (RS.AN, RS.CO, RS.MI, RS.RP), Recover (RC.CO, RC.IM, RC.RP)

**7.1 Secure Execution** (DS.SE): CBRN devices MUST have the ability to respond to CWMD device level cybersecurity events. CWMD MUST have a policy that conforms CBRN devices to enable response features or functions that support event monitoring requirements.
**Related NIST 800-213A:** LA: ROL(4), DS: EXE(1)(2)(3), RSC(2)(3)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**7.1.1** Separate user functionality that includes the user interface services from the system management functionality. Related Control: SC-2 (Mod/High)

**7.1.2** Maintain a separation of the executing processes for the device that includes but is not limited to logically separating CBRN software and firmware from other software, firmware, and data that be connected and limit access to potentially untrusted software to other system resources. Related Control: SC-39 (Low/Mod/High)

**7.2 Secure Communication** (DS.SC): The CBRN device MUST have documentation that details how the device is expected to behave and how it establishes and/or terminates network connections. Also included should be the application of a secure mechanism for initiating or terminating communications.
**Related NIST 800-213A:** CS: EIM(6), DS: COM(2)(3)(4)(5)(7)(8)(9)(10)(11), RSC(9), DP: STX(2)(4)

***Best Practices that may be necessary/MUST have the ability to:***

**7.2.1** Connect to external networks or other systems through a managed interface that consists of boundary protection devices (e.g., gateways, routers, firewalls, etc.) that adhere to CWMD security and privacy policies. Related Control: SC-7 (Low/Mod/High)
**7.2.2** Identify the protocol format for CBRN device uses and adhere to the protocol format to enable the detection of vulnerabilities or anomalies. Related Control: SC-7(17)
**7.2.3** Protect data transmission that could include encryption techniques identified by CWMD policies. Related Control: SC-8 (Mod/High)
**7.2.4** Terminate a network connection at the end of a communications session or a period of inactivity defined by CWMD policies. Related Control: SC-10 (Mod/High)
**7.2.5** Ensure that transmitted security and privacy attributes associated with the CBRN device information have not been modified in an unauthorized manner. Related Control: SC-16(2)
**7.2.6** Verify the authenticity and integrity of data being received from other sources. Related Control: SC-21 (Low/Mod/High)
**7.2.7** Include resources for the protection of communications and the validity of transmitted information. Related Control: SC-23 (Mod/High)
**7.2.8** Include protections for hardware-based write protection that cannot be disabled without proper permission. Related Control: SC-51

**7.3 Secure Resource Usage in a Degraded State** (DS.SRUD): The CBRN device MUST have the ability to function in a degraded state to ensure that any information is not lost, or it should have the capability to be shut down and taken off the network until the device has been restored to a known good state.
**Related NIST 800-213A:** DS: RSC(1)(5)(6)(7)(8), OPS(3)(4)(5)(6)(8), DIN(5)

***Best Practices that may be necessary/MUST have the ability to:***

**7.3.1** Enter a safe mode of operation when abnormal behaviors are detected or observed with a CBRN device with limited network access until, at a predetermined time defined by CWMD, the device can be deemed safe for normal use. Related Control: CP-12
**7.3.2** Prevent the unauthorized or unintended transfer of information from shared resources. This includes encrypted information transfers from CBRN devices. Related Control: SC-4 (Mod/High)
**7.3.3** If applicable, include protections that can filter certain types of packets to protect system components on internal networks from being affected by or source of denial-of-service attacks. Related Control: SC-5 (Low/Mod/High)
**7.3.4** The CBRN device should fail to a known state defined by CWMD while preserving data confidentiality, integrity, and availability of the device if such a failure occurs. CWMD should define the system failures and outline processes and procedures for the restoration of the device. Related Control: SC-24 (High)

**7.3.5** The CBRN device should have reliable hardware protection against reprogramming the memory, from the point of the initial writing to the insertion of the memory into the CBRN device. Related Control: SC-34

**7.3.6** Outline the fail-safe procedures the user can follow if an indicated failure occurs with the CBRN device. Related Control: SI-17

**7.4 Device Integrity** (DS.DI): Enforce protection mechanisms against unauthorized changes to the hardware or software of CBRN devices.
**Related NIST 800-213A:** DS: DIN(1)(3)

***Best Practices that may be necessary/MUST have the ability to:***

***7.4.1*** Perform security and privacy checks on the CBRN device prior to the establishment of network connections. Related Control: CA-9(1)

**7.4.2** Employment of anti-tamper technologies, tools, and techniques should be applied throughout the system development lifecycle. Related Control: SR-9(1) (High)

**7.5 Secure Network Onboarding Support** (DS.SNOS)**:** Use secure network onboarding technologies to support the secure network onboarding of CBRN devices.
**Related NIST 800-213A:** DS: ONB(2)(3); CS: EIM(6)

***Best Practices that may be necessary/MUST have the ability to:***

**7.5.1** Employ password authentication mechanisms that include: A list of commonly used, expected, or compromised passwords and the list should be updated periodically. Related Control: IA-5(1) (Low/Mod/High)

a. When users of the CBRN device create or update passwords, the passwords are not found on the commonly used, expected, or compromised passwords list.
b. All passwords should be cryptographically protected on all CBRN devices.

**7.5.2** The CRBN device should only connect to external networks or other systems through a managed interface that consists of boundary protection devices (e.g., gateways, routers, firewalls, etc.) that adhere to CWMD security and privacy policies. Related Control: SC-7 (Low/Mod/High)

**7.6 Secure Device Operation** (DS.SDO)**:** Employ internal and external safeguards for the secured use of CBRN devices in various operational states.
**Related NIST 800-213A:** DS: RSC(6), OPS(3)(4)(6)(7)

***Best Practices that may be necessary/MUST have the ability to:***

**7.6.1** The CBRN device should recover and reconstitute to a known good state within a period of time defined by CWMD policies and procedures after a disruption, compromise, or failure of the CBRN device. Related Control: CP-10 (Low/Mod/High)

**7.6.2** The CBRN device should automatically disable the system if security violations are detected (e.g., cyber-attack, exfiltration of device information, errors in the programming software, etc.). Related Control: IR-4(5)

# Appendix C – CWMD Cybersecurity Best Practices and Controls Table

**Summary:** Appendix C provides the CWMD cybersecurity best practices controls summary for CBRN devices, the related security control mapping, the FIPS 199 security impact levels (Low/Mod/High), and the NIST informative references corresponding to the Cybersecurity Framework categories and sub-categories.

**Purpose:** Appendix C can be used by subject matter experts as a security control checklist to identify and benchmark which controls have been implemented on CBRN devices in their operating environment across three criteria (e.g., fully, partially, or not Implemented); assessing implementations and establishing benchmarks can also be referenced by program managers to document CBRN device security coverages. All Controls outlined in Appendix C are derived from NIST SP 800-53, Revision 5, Security and Privacy Controls for Information Systems and Organizations and NIST SP 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog security controls.

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| **1 Device Identification:** MUST identify CBRN devices for multiple purposes (e.g., asset management, vulnerability management, access management, data | **1.1 Device Identifier:** A unique device identifier initiates the ability to identify system elements for monitoring CBRN devices and manage assets. The CBRN | **1.1.1** Employ a mechanism to uniquely identify and authenticate CBRN devices before establishing a network connection (local, remotely). Related NIST 800-53R5 Controls: IA-3 (Mod/High) | DI.DI-1.1(1) | DI: IMS(1), IMS(2), AID(1), AID(4), DAS(1), DAS(2), PID(1) | IA-3 | | x | x | CSF: PR.AC-1, PR.AC-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| protection, and incident detection) and in multiple ways using logical identifiers and device behavior identification to meet organizational requirements. | devices should incorporate a unique identifier that can be used to identify the device logically. This also enables a linkage to the person or processes assigned to use the device. | **1.1.2** Select an identifier that can be assigned to the roles, services, and individuals for CBRN devices. Related NIST 800-53R5 Controls: IA-4 (Low/Mod/High) | DI.DI-1.1(2) | DI: IMS(3) | IA-4 | x | x | x | CSF: PR.AC-1, PR.AC-6 | | | |
| | | **1.1.3** Unique device identifiers should not be reused for any service. Related NIST 800-53R5 Controls: IA-4 (Low/Mod/High) | DI.DI-1.1(3) | DI: IMS(3) | IA-4 | x | x | x | CSF: PR.AC-1, PR.AC-6 | | | |
| | **1.2 Device Identity Actions:** The differentiation of CBRN devices can help provide assurance on the applied security controls by monitoring the device actions | **1.2.1** Create a list of event types to be monitored and have mechanisms in place for auditing and record retention. This is an important step to identify a root cause of a problem. Related Control: AU-2 (Low/Mod/High) | DI.DIA-1.2(1) | DI: AID(2) | AU-2 | x | x | x | CSF: PR.PT-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | based on the assigned identity. | **1.2.2** Implement an automated mechanism for tracking assets by location and responsible individuals of CBRN devices. CWMD should have the capability to rapidly respond to a compromise and breach and apply mitigations actions in a timely manner. Related Control: CM-8(8) (Low/Mod/High) | DI.DIA-1.2(2) | DI: AID(3), AID(4) | CM-8 | x | x | x | CSF: ID.AM-1, ID.AM-2, PR.DS-3, DE.CM-7 | | | |
| | | **1.2.3** Enforce approved authorizations for logical access to information and system resources in accordance with applicable CWMD access control policies. Related NIST | DI.DIA-1.2(3) | DI: AID(1) | AC-3 | x | x | x | CSF: PR.AC-4, PR.PT-3 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | 800-53R5 Controls: AC-3 (Low/Mod/High) | | | | | | | | | | |
| | | **1.2.4** Invoke internal monitoring capabilities or deploy CBRN monitoring devices strategically within the system to collect appropriate CWMD-determined essential information and at ad hoc locations within the system to track specific types of transactions of interest. Related NIST 800-53R5 Controls: SI-4 (Low/Mod/High) | DI.DIA-1.2(4) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.CO-3, RS.AN-1 | | | |
| | | **1.2.5** Analyze detected events and anomalies. Related NIST 800-53R5 Controls: SI-4 (Low/Mod/High) | DI.DIA-1.2(5) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | | | | | | | | DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 | | | |
| | | **1.2.6** Adjust the level of system monitoring activity when there is a change in risk to organizational operations and assets, individuals, other organizations, or the nation. Related NIST 800-53R5 Controls: SI-4 (Low/Mod/High) | DI.DIA-1.2(6) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | | | | | | | | DE.DP-5, RS.AN-1 | | | |
| | **1.3 Authentication Support:** CWMD should be able to support CBRN interfaced device authentication. The CBRN device may need to authenticate its identify with other systems and other systems elements. | **1.3.1** Limited the number of CBRN device connections based on mission needs. Related NIST 800-53R5 Controls: IA-3 (Mod/High) | DI.AS-1.3(1) | DI: IMS(1), IMS(2), AID(1), AID(4), DAS(1), DAS(2), PID(1) | IA-3 | | x | x | CSF: PR.AC-1, PR.AC-7 | | | |
| | | **1.3.2** Enable bi-directional authentication that is cryptographically based. Related NIST 800-53R5 Controls: IA-3 (Mod/High) | DI.AS-1.3(2) | DI: IMS(1), IMS(2), AID(1), AID(4), DAS(1), DAS(2), PID(1) | IA-3 | | x | x | CSF: PR.AC-1, PR.AC-7 | | | |
| | **1.4 Physical Identifiers:** CWMD should be able to apply a mechanism to identify the CBRN device on | **1.4.1** Periodically verify physical identifiers and logical identifiers are properly incorporated under asset management control. | DI.PI-1.4(1) | DI: IMS(1), IMS(2), AID(1), AID(4), DAS(1), DAS(2), PID(1) | IA-3 | | x | x | CSF: PR.AC-1, PR.AC-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | physical attributes internally or externally unique to each device. | Related NIST 800-53R5 Controls: IA-3 (Mod/High) | | | | | | | | | | |
| **2 Device Configuration:** The CBRN device should have the capability to be configured through logical and/or physical interfaces to meet CWMD requirements. This supports vulnerability management, access management, data protection, and incident detection. CWMD should be able to implement protective | 2.1 Privileged Access Configurations: The CBRN device should support the ability to apply logical access privilege settings for authorized users to ensure the integrity of CBRN access and usage. (ORGANIZATIONAL 800-213A and 800-53 users or processes acting on behalf of organizational users). | **2.1.1** Uniquely identify and authenticate users and associate that unique identification with CBRN device processes acting on behalf of those users. Related NIST 800-53R5 Controls: IA-2 (Low/Mod/High) | DC.PAC-2.1(1) | LA: AUN(1), AUZ(1), AUZ(2) | IA-2 | x | x | x | CSF: PR.AC-1, PR.AC-6, PR.AC-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| measures to ensure the confidentiality, integrity, and availability of the configurations. | **2.2 Authentication and Authorization:** Must have the ability to limit any changes to CBRN devices by employing system policies for authentication and authorization. Related NIST 800-53R5 Controls: AC-3, CM-5 | **2.2.1** Enforce approved authorizations for physical access to information and system resources in accordance with applicable CWMD access control policies. Related NIST 800-53R5 Controls: AC-3, CM-5 (Low/Mod/High) | DC.AA-2.2(1) | DI: AID(1) | AC-3, CM-5 | x | x | x | CSF: PR.AC-4, PR.PT-3 | | | |
| | | **2.2.2** Define, document, approve, and enforce physical and logical access restrictions associated with changes to the CBRN device. Related NIST 800-53R5 Controls: CM-5 (Low/Mod/High) | DC.AA-2.2(2) | DC: PRV(1), AUT(1), INT(1), CTL(2), CTL(4) | CM-5 | x | x | x | CSF: PR.IP-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | **2.3 Interface Configuration:** Only authorized CWMD personnel can configure aspects of CBRN devices. | **2.3.1** Permit authorized individuals to access CBRN devices for purpose of initiating changes. Access restrictions can include:<br>a. Physical and logical access<br>b. Software libraries<br>c. Abstract layers<br>d. Change windows (times allocated by CWMD)<br>Related Control: CM-5 (Low/Mod/High) | DC.IC-2.3(1) | DI: AID(1) | AC-3 | x | x | x | CSF: PR.AC-4, PR.PT-3 | | | |
| | **2.4 Display Restrictions:** The CBRN device MUST have the ability to configure content to be displayed on a device. | **2.4.1** Display system use notification message or banner prior to granting access to U.S. Government CBRN systems and/or devices. Related NIST 800-53R5 Controls: AC-8 (Low/Mod/High) | DC.DR-2.4(1) | DC: DSP(1) | AC-8 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **2.4.2** Device usage should be monitored, recorded, and subject to audit Related Control: AC-8 (Low/Mod/High) | DC.DR-2.4(2) | DC: DSP(1) | AC-8 | x | x | x | CSF: N/A | | | |
| | | **2.4.3** Prohibit unauthorized use of the CBRN device subject to criminal and civil penalties. Related NIST 800-53R5 Controls: AC-8 (Low/Mod/High) | DC.DR-2.4(3) | DC: DSP(1) | AC-8 | x | x | x | CSF: N/A | | | |
| | | **2.4.4** Display message that use of the device indicates consent to monitoring and recording. Related NIST 800-53R5 Controls: AC-8 (Low/Mod/High) | DC.DR-2.4(4) | DC: DSP(1) | AC-8 | x | x | x | CSF: N/A | | | |
| | | **2.4.5** Establish standard lengths of time when terminating user | DC.DR-2.4(5) | DC: DSP(1) | AC-12(2) | | | | CSF: PR.PT-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | sessions on CBRN devices, based on the needs of the mission. Related Control: AC-12(2) | | | | | | | | | | |
| | **2.5 Device Configuration Control:** Have all baseline configurations for CBRN devices documented, maintained, and controlled by CWMD. | **2.5.1** Include the security and privacy control implementations on CBRN device components that include connectivity, operational components, and communications serve as the basis for future builds, releases, or changes to the devices. Related Control: CM-2 (Low/Mod/High) | DC.DCC-2.5(1) | DC: CTL(1), CTL(2) | CM-2 | x | x | x | CSF: PR.DS-7, PR.IP-1, DE.AE-1 | | | |
| | | **2.5.2** Document the baseline configurations for operational procedures, information about | DC.DCC-2.5(2) | DC: CTL(1), CTL(2) | CM-2 | x | x | x | CSF: PR.DS-7, PR.IP-1, DE.AE-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | the system components, and network connectivity to identify any unnecessary or unwanted changes. Related NIST 800-53R5 Controls: CM-2 (Low/Mod/High) | | | | | | | | | | |
| | | **2.5.3** Determine and document the types of changes to the CBRN devices. Related NIST 800-53R5 Controls: CM-3 (Mod/High) | DC.DCC-2.5(3) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |
| | | **2.5.4** Review proposed configuration-controlled changes to the CBRN device and approve or disapprove such changes with explicit consideration for security and privacy impact analyses. | DC.DCC-2.5(4) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | Related NIST 800-53R5 Controls: CM-3 (Mod/High) | | | | | | | | | | |
| | | **2.5.5** Document configuration change decisions associated with the CBRN device. Related NIST 800-53R5 Controls: CM-3 (Mod/High) | DC.DCC-2.5(5) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |
| | | **2.5.6** Retain records of configuration-controlled changes. Related NIST 800-53R5 Controls: CM-3 (Mod/High) | DC.DCC-2.5(6) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |
| | | **2.5.7** Monitor and review activities associated with configuration-controlled changes to the system. Related NIST 800-53R5 Controls: CM-3 (Mod/High) | DC.DCC-2.5(7) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **2.5.8** Establish and document configuration settings for components employed within the CBRN device that reflect the most restrictive mode consistent with operational requirements. Related NIST 800-53R5 Controls: CM-6 (Low/Mod/High) | DC.DCC-2.5(8) | DC: CTL(4) | CM-6 | x | x | x | CSF: PR.IP-1 | | | |
| | | **2.5.9** Monitor and control changes to the configuration settings in accordance with CWMD policies and procedures. Related NIST 800-53R5 Controls: CM-6 (Low/Mod/High) | DC.DCC-2.5(9) | DC: CTL(4) | CM-6 | x | x | x | CSF: PR.IP-1 | | | |
| **3 Data Protection:** Data protection on a CBRN device | **3.1 Cryptography:** The CBRN device | **3.1.1** Prevent unauthorized or unintended transfer | DP.C-3.1(1) | DS: RSC(1) | SC-4 | | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| supports CWMD cybersecurity needs and goals such as access management, system and organizational data protection, and incident detection. Confidentiality, availability, and integrity of data is central to cybersecurity. | MUST have the ability to employ secured mechanisms to ensure the confidentiality of data at rest and in transit, authentication for users of CBRN devices, and to ensure secured communications when in the field. | of information from shared resources. This includes encrypted information transfers from CBRN devices. Related Control: SC-4 (Mod/High) | | | | | | | | | | |
| | | **3.1.2** Use cryptography solutions to protect CBRN information (e.g., data, configurations, locations, etc.) by using NSA approved cryptography or FIPS validated cryptography. Related Control: SC-13 (Low/Mod/High) | DP.C-3.1(2) | DP: CRY(1), CRY(2),CRY(3), CRY(4), CRY(5), KEY(1) | SC-13 | x | x | x | CSF: N/A | | | |
| | **3.2 System and Communications Protection:** CWMD should be able to demonstrate the | **3.2.1** Implement subnetworks for publicly accessible system components that are physically separated from | DP.SCP-3.2(1) | CS: EIM(6) | SC-7 | x | x | x | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | ability to securely initiate and terminate communications between CBRN devices and supporting systems. | internal organizational networks and should only be connected through managed interfaces with boundary protection in accordance with CWMD security privacy architectures (e.g., firewalls, gateways, routers, encrypted tunnels, etc.). Related Control: SC-7 (Low/Mod/High) | | | | | | | | | | |
| | | **3.2.2** Take precautions to limit the number of external connections to CBRN devices. Related Control: SC-7(3) (Mod/High) | DP.SCP-3.2(2) | N/A | SC-7(3) | | x | x | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **3.2.3** Protect CBRN devices that have the capability to allow additional physical connections to the device (e.g., USB, ethernet). There also should be protections in place that would disallow unauthorized users from physical access to the device (card reader, locks, boxes, etc.). Related Control: SC-7(14) | DP.SCP-3.2(3) | N/A | SC-7(14) | | | | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |
| | | **3.2.4** Prohibit the direct connection of CBRN devices to external networks (e.g., virtual interface, internet). Related Control: SC-7(25) | DP.SCP-3.2(4) | N/A | SC-7(25) | | | | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |
| | | **3.2.5** Prohibit the direct connection of CRBN device to a public network and | DP.SCP-3.2(5) | N/A | SC-7(28) | | | | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | apply configuration management of the device when commissioned. Related Control: SC-7(28) | | | | | | | | | | |
| | **3.3 Secure Storage:** Some CBRN devices may have the capability to store data during and after use in the field. MUST have the ability to enable secure device data storage for CBRN devices. | **3.3.1** Ensure that there is a system backup of CBRN devices for restoration that includes security-related documentation, system-level information, and user-level information. Related Control: CP-9 (Low/Mod/High) | DP.SS-3.3(1) | DP: STO(3) | CP-9 | x | x | x | CSF: PR.IP-4 | | | |
| | | **3.3.2** Ensure that the implementation of cryptographic mechanisms is in place from information backed up from CBRN | DP.SS-3.3(2) | DP: STO(3) | CP-9(8) | | x | x | CSF: PR.IP-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | devices. Related Control: CP-9(8) (Mod/High) | | | | | | | | | | |
| | | **3.3.3** Ensure sanitization mechanisms are commensurate with security or classification of information stored before decommissioning or disposal of CBRN devices. Related Control: MP-6 (Low/Mod/High) | DP.SS-3.3(3) | DP: STO(4) | MP-6 | x | x | x | CSF: PR.DS-1, PR.DS-3, PR.IP-6 | | | |
| | | **3.3.4** Protect information at rest when data has been received from CBRN devices after use. Related Control: SC-28 (Mod/High) | DP.SS-3.3(4) | DP: STO(1), STO(2) | SC-28 | | x | x | CSF: PR.DS-1 | | | |
| | | **3.3.5** Apply cryptographic applications to ensure the | DP.SS-3.3(5) | DP: STX(1), STX(3) | SC-8(1) | | x | x | CSF: PR.DS-2 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | confidentiality of the CBRN data and to detect any changes to the information during transmission. Related Control: SC-8(1) (Mod/High) | | | | | | | | | | |
| **4 Logical Access to Interfaces:** Establish requirements for authentication and identification, configuration, and display requirements to support cybersecurity needs and goals (e.g., vulnerability management, access management, data protection, incident detection). Some CBRN devices may have access interfaces that | **4.1 Authentication Support and Configuration:** Support authentication methods for physical and logical access to CBRN devices. | **4.1.1** Implement multi-factor authentication for remote commands to ensure that CBRN devices are protected against unauthorized commands. Related Control: AC-17(10) | LAI.ASC-4.1(1) | LA: AUN(4) | AC-17(10) | | | | CSF: PR.AC-3, PR.PT-4 | | | |
| | | **4.1.2** Incorporate identification and authentication requirements for the use of CBRN devices and the transfer of CBRN data to ensure accountability and traceability of users. Related Control: IA-2 (Low/Mod/High) | LAI.ASC-4.1(2) | LA: AUN(1), AUZ(1), AUZ(2) | IA-2 | x | x | x | CSF: PR.AC-1, PR.AC-6, PR.AC-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| could include physical and logical components to support its management and use. | | **4.1.3** Disable the usage of CBRN devices when they are not in use after a designated time period until the user is able to reauthenticate their credentials. Related Control: AC-2(5) (Mod/High) | LAI.ASC-4.1(3) | LA: ACF(1) | AC-2(5) | | x | x | CSF: PR.AC-4, DE.CM-3 | | | |
| | | **4.1.4** Disable access and ensure the integrity of the CBRN device has not been compromised, if the security attributes of the CBRN device have changed after being configured by CWMD. Related Control: AC-3(8) | LAI.ASC-4.1(4) | LA: ACF(3) | AC-3(8) | | | | CSF: PR.AC-4, PR.PT-3 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **4.1.5** Impose a limit on how many unsuccessful logins are attempted by the user. Once the limit has been reached, the CBRN device should be locked for a designated amount of time defined by CWMD. If the maximum number of unsuccessful logins have exceeded what has been defined by CWMD, the device should lock or disable until it is released by an authority designated by CWMD. Related Control: AC-7 (Low/Mod/High) | LAI.ASC-4.1(5) | LA:ACF(1) | AC-7 | x | x | x | CSF: N/A | | | |
| | **4.2 Role Management:** Establish unique user accounts for | **4.2.1** Establish an accountability mechanism that enables the | LAI.RM-4.2(1) | LA: ROL(1), ROL(2), ROL(3), ROL(4), ROL(6) | AC-2 | x | x | x | CSF: PR.AC-4, DE.CM-3 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | CBRN devices in use to ensure the correct personnel can use, handle, and operate the device based on configured CWMD user information. | monitoring of users that have control and use a CBRN device to ensure the principle of least privilege. Related Control: AC-2 (7) (Low/Mod/High) | | | | | | | | | | |
| | | **4.2.2** Provide an enforcement mechanism to prevent unauthorized access or changes to a CBRN device after the initial installation of the CBRN software. Related Control: AC-3(12) | LAI.RM-4.2(2) | N/A | AC-3(12) | | | | CSF: PR.AC-4, PR.PT-3 | | | |
| | | **4.2.3** Enforce the least privilege for the use of CRBN devices, allowing only authorized personnel to use or make changes to the CBRN device. Related Control: AC-6 (Mod/High) | LAI.RM-4.2(3) | LA:ROL(5),LA:IFC(4),LA:IFC(5) | AC-6 | | x | x | CSF: PR.AC-4, PR.DS-5 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **4.2.4** Employ a mechanism to separate user functionality from the management of the CBRN device to prevent unauthorized changes. Related Control: SC-2 (Mod/High) | LAI.RM-4.2(4) | LA: ROL(4)<br>DS: EXE(2), EXE(3) | SC-2 | | x | x | CSF: N/A | | | |
| | **4.3 Limitations on Device Usage:** Establish restrictions or limitations for how CBRN devices can be used by internal or external users. | **4.3.1** Determine whether access authorizations assigned to a sharing partner match user restrictions and information access to the CRBN device. Related Control: AC-21 (Mod/High) | LAI.LDU-4.3(1) | LA: ROL(8), LDU(1), XCN(1), XCN(2), XCN(3) | AC-21 | | x | x | CSF: PR.IP-8 | | | |
| | **4.4 External Connections:** Identify the security best practices for external connections | **4.4.1** Establish identification mechanisms for external connections to CBRN devices to ensure no unauthorized | LAI.EC-4.4(1) | N/A | AC-20 | x | x | x | CSF: ID.AM-4, PR.AC-3 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | when CRBN devices are operating on external networks. Some CBRN devices may need external connections that could include (e.g., wireless, Bluetooth). | connections are established without proper permission or security. Related Control: AC-20 (Low/Mod/High) | | | | | | | | | | |
| | | **4.4.2** Enforce restrictions on information sharing based on access restrictions and security configurations for external connections. Related Control: AC-21(1) | LAI.EC-4.4(2) | N/A | AC-21(1) | | | | CSF: PR.IP-8 | | | |
| | | **4.4.3** Employ cryptographic mechanisms to protect the confidentiality and integrity of transmitted information from the CBRN device. Related Control: SC-8 (Mod/High) | LAI.EC-4.4(3) | DP: STX(2), STX(4) | SC-8 | | x | x | CSF: PR.DS-2 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | **4.5 Interface Control:** MUST have the ability to establish security controls for any connection to and from CBRN devices. | **4.5.1** Enforce the principle of least privilege for the use of CRBN devices on any connection outside the control of CWMD. Related Control: AC-6 (Mod/High) | LAI.IC-4.5(1) | LA:ROL(5),LA:IFC(4),LA:IFC(5) | AC-6 | | x | x | CSF: PR.AC-4, PR.DS-5 | | | |
| | | **4.5.2** Document rationale for remote access to the CBRN device in the security plan. Related Control: AC-17(4) (Mod/High) | LAI.IC-4.5(2) | LA: ACF(2), IFC(1) | AC-17(4) | | x | x | CSF: PR.AC-3, PR.PT-4 | | | |
| | | **4.5.3** Establish the configuration requirements, connection requirements, and implementation guidance for wireless capabilities with CBRN devices, in addition to the authorization of wireless access to the | LAI.IC-4.5(3) | LA: IFC(8) | AC-18 | x | x | x | CSF: PR.PT-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | CRBN device, before allowing connections. Related Control: AC-18 (Low/Mod/High) | | | | | | | | | | |
| | | **4.5.4** Establish an authentication and encryption mechanism that aligns with CWMD policies to protect wireless access and connection with a CBRN device. AC-18(1) (Mod/High) | LAI.IC-4.5(4) | LA: IFC(13), IFC(14), IFC(15) | AC-18(1) | | x | x | CSF: PR.PT-4 | | | |
| | | **4.5.5** Disable any wireless networking capabilities embedded within CRBN system components before issuance and deployment. Related Control: AC-18(3) (Mod/High) | LAI.IC-4.5(5) | N/A | AC-18(3) | | x | x | CSF: PR.PT-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **4.5.6** Define, document, approve, and enforce physical and logical access restrictions associated with changes to the CBRN device. Related Control: CM-5 (Low/Mod/High) | LAI.IC-4.5(6) | N/A | CM-5 | x | x | x | CSF: PR.IP-1 | | | |
| | | **4.5.7** Remove unused or unnecessary software and disable unused or unnecessary physical and logical ports and protocols to prevent unauthorized connection of components, transfer of information, and tunneling. Related Control: CM-7 (Low/Mod/High) | LAI.IC-4.5(7) | DC: PRV(1), AUT(1), INT(1), CTL(2), CTL(4), | CM-7 | x | x | x | CSF: PR.IP-1, PR.PT-3 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| **5 Software Update:** Updates for CBRN devices are essential for vulnerability management. Updates can correct operational problems with the software or firmware. Support mechanisms are in place for updates that improve availability, reliability, performance, and other aspects of CBRN operations. | **5.1 Update Capabilities:** Update software within the device or through its interface with proper security in place. | **5.1.1** Develop and document an audit and accountability policy that addresses the purpose of contributing to security and privacy assurance based on CWMD mission or CRBN device specific policies and procedures. Related Control: AU-1 (Low/Mod/High) | SU.UC-5.1(1) | SU: UPD(2) | AU-1 | x | x | x | CSF: PR.PT-1 | | | |
| | | **5.1.2** Incorporate a mechanism to test, review, and identify any changes to a CBRN device, including system upgrades and modifications. This can include any changes to baseline configurations, operational procedures, | SU.UC-5.1(2) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | configuration settings for CBRN device components, remediation of vulnerabilities, and unscheduled or unauthorized changes. Related Control: CM-3 (Mod/High) | | | | | | | | | | |
| | | **5.1.3** Enforce access restrictions for changes to a CBRN device that should include physical and logical access controls by defining and documenting any associated changes to the CBRN device. Related Control: CM-5 (Low/Mod/High) | SU.UC-5.1(3) | DC: PRV(1), AUT(1), INT(1), CTL(2), CTL(4), | CM-5 | x | x | x | CSF: PR.IP-1 | | | |
| | | **5.1.4** Prevent the installation of any software or firmware components on a CBRN device without | SU.UC-5.1(4) | N/A | CM-14 | | | | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | verification that it has been recognized and approved by CWMD. Related Control: CM-14 | | | | | | | | | | |
| **6 Cybersecurity State Awareness:** Prevent the unauthorized or unintended transfer of information from trusted CBRN devices. Support vulnerability management, incident detection and investigation of potential compromises, and troubleshoot from a known operational state. Capture critical CBRN device information from logging and auditing, depending on the device | **6.1 Access to Event Information:** MUST have the ability to access CBRN device state information and the ability to collect and make data available when necessary. | **6.1.1** Retain audit records based on established records retention policies to support post-incident investigations. Related Control: AU-11 (Low/Mod/High) | CSA.AEI-6.1(2) | CS: AEI(2), RDL(3), LSR(2), LSR(3) | AU-11 | x | x | x | CSF: N/A | | | |
| | | **6.1.2** Create a list of event types to be monitored, have mechanisms in place for logging and auditing, and generate and retain audit records for select CBRN devices. This is an important step to identify a root cause of a problem. Related Control: AU-12 (Low/Mod/High) | CSA.AEI-6.1(1) | CS: AEI(2) | AU-12 | x | x | x | CSF: DE.CM-1, DE.CM-3. DE.CM-7, PR.PT-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| design, use case, or other consideration. | | **6.1.3** Monitor unauthorized local, network, and remote connections and detect cyberattacks and indicators of potential attacks. Related Control: SI-4 (Low/Mod/High) | CSA.AEI-6.1(3) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 | | | |
| | | **6.1.4** Identify unauthorized use of the system using established techniques and methods. Related Control: SI-4 (Low/Mod/High) | CSA.AEI-6.1(4) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | | | | | | | | DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 | | | |
| | | **6.1.5** Analyze detected events and anomalies from external and internal monitoring within the system. Related Control: SI-4 (Low/Mod/High) | CSA.AEI-6.1(5) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.1.6** Adjust the level of system monitoring activity when there is a change in risk to system operations, CBRN devices, individuals, other organizations, or the nation. Related Control: SI-4 (Low/Mod/High) | CSA.AEI-6.1(6) | DI: AID(2) | SI-4 | x | x | x | CSF: ID.RA-1, PR.DS-5, PR.IP-8, DE.AE-1, DE.AE-2, DE.AE-3, DE.AE-4, DE.CM-1, DE.CM-4, DE.CM-5, DE.CM-6, DE.CM-7, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, RS.AN-1 | | | |
| | **6.2 Event Identification & Monitoring:** Provide event identification and monitoring capabilities and/or support event | **6.2.1** Deploy a mechanism for monitoring open-source information for evidence of unauthorized disclosure or data leakage attributed to CBRN-related device | CSA.EIM-6.2(1) | CS: EIM(5) | AU-13 | | | | CSF: DE.CM-3, PR.DS-5, PR.PT-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | identification and monitoring tools interfacing with CBRN devices. | information. Related Control: AU-13 | | | | | | | | | | |
| | | **6.2.2** Define personnel, roles, and actions to support notification procedures whenever information disclosure is discovered. Related Control: AU-13 | CSA.EIM-6.2(2) | CS: EIM(5) | AU-13 | | | | CSF: DE.CM-3, PR.DS-5, PR.PT-1 | | | |
| | | **6.2.3** Develop a system-level continuous monitoring strategy that includes establishing CBRN device-level metrics, frequency of occurrence for control assessment effectiveness, correlation and analysis of information generated, response | CSA.EIM-6.2(3) | CS: EIM(1), EIM(2), EIM(4), EIM(5), EIM(6), EIM(7), EIM(8), EIM(9), EIM(10) | CA-7 | x | x | x | CSF: ID.RA-1, PR.IP-7, PR.IP-8, DE.AE-2, DE.AE-3, DE.CM-1, DE.CM-2, DE.CM-3, DE.CM-6, DE.CM-7, DE.DP-1, DE.DP-2, DE.DP-3, DE.DP-4, DE.DP-5, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | actions to address the results of control assessment analysis and reporting the security and privacy status of CBRN devices to appropriate CWMD personnel. Related Control: CA-7 (Low/Mod/High) | | | | | | | RS.CO-3, RS.AN-1, RS.MI-3 | | | |
| | | **6.2.4** Determine, document, and retain records of the changes to CBRN devices that are under configuration control. Related Control: CM-3 (Mod/High) | CSA.EIM-6.2(4) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |
| | | **6.2.5** Consider the security and privacy implications before making decisions to approve or disapprove proposed configuration control | CSA.EIM-6.2(5) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | changes. Related Control: CM-3 (Mod/High) | | | | | | | | | | |
| | | **6.2.6** Implement approved configuration control changes to CBRN devices and perform associated monitoring and review activities. Related Control: CM-3 (Mod/High) | CSA.EIM-6.2(6) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |
| | | **6.2.7** Provide oversight for configuration change control activities to CBRN devices, in accordance with CWMD mission assurance levels and protection conditions. Related Control: CM-3 (Mod/High) | CSA.EIM-6.2(7) | DC: CTL(1) | CM-3 | | x | x | CSF: PR.IP-1, PR.IP-3, DE.CM-1, DE.CM-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.2.8** Define, document, approve, and enforce physical and logical access restrictions associated with changes to CBRN devices and the systems they support. Related Control: CM-5 (Low/Mod/High) | CSA.EIM-6.2(8) | DC: PRV(1), AUT(1), INT(1), CTL(2), CTL(4) | CM-5 | x | x | x | CSF: PR.IP-1 | | | |
| | | **6.2.9** Enforce access restrictions for CBRN devices, where applicable, using automated mechanisms and automatically generate audit records of the enforcement actions. Related Control: CM-5(1) (High) | CSA.EIM-6.2(9) | N/A | CM-5(1) | | | x | CSF: PR.IP-1 | | | |
| | | **6.2.10** Establish, document, and implement configuration settings | CSA.EIM-6.2(10) | DC: CTL(4) | CM-6 | x | x | x | CSF: PR.IP-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | for CBRN devices employed within the system that reflect the most restrictive mode consistent with operational requirements. Related Control: CM-6 (Low/Mod/High) | | | | | | | | | | |
| | | **6.2.11** Monitor and control changes to the configuration settings of CBRN devices, in accordance with organizational policies and procedures. Related Control: CM-6 (Low/Mod/High) | CSA.EIM-6.2(11) | DC: CTL(4) | CM-6 | x | x | x | CSF: PR.IP-1 | | | |
| | | **6.2.12** Uniquely identify and authenticate users and associate that unique identification with CBRN device processes acting on | CSA.EIM-6.2(12) | LA: AUN(1), AUZ(1), AUZ(2) | IA-2 | x | x | x | CSF: PR.AC-1, PR.AC-6, PR.AC-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | behalf of those users. Related Control: IA-2 (Low/Mod/High) | | | | | | | | | | |
| | | **6.2.13** Implement subnetworks for publicly accessible system components that are physically separated from internal organizational networks and should only be connected through managed interfaces with boundary protection in accordance with CWMD security privacy architectures (e.g., firewalls, gateways, routers, encrypted tunnels, etc.). Related Control: SC-7 (Low/Mod/High) | CSA.EIM-6.2(13) | CS: EIM(6) | SC-7 | x | x | x | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.2.14** Prohibit remote activation of collaborative computing devices and applications (e.g., cameras, microphones, etc.) except where remote activation is authorized. Collaborative devices and applications should include signals to indicate when they are activated. Related Control: SC-15 (Low/Mod/High) | CSA.EIM-6.2(14) | CS: EIM(8), EIM(9), EVR(5) | SC-15 | x | x | x | CSF: PR.AC-3 | | | |
| | | **6.2.15** Prohibit the use of individual CBRN devices from possessing other sensors and/or sensing capabilities (e.g., mobile devices, cellular phones, smart phones, tablets, etc.) that are | CSA.EIM-6.2(15) | CS: EIM(10), EVR(6) | SC-42 | | | | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | designated for CWMD-defined operating environments, facilities, or systems. Related Control: SC-42 | | | | | | | | | | |
| | | **6.2.16** Configure CBRN devices so that only data or information collected by the CBRN sensors and/or sensing capabilities is reported to authorized individuals or roles. Related Control: SC-41(1) | CSA.EIM-6.2(16) | N/A | SC-41(1) | | | | CSF: N/A | | | |
| | **6.3 Event Response:** Enable response features or functions that support event monitoring requirements. | **6.3.1** Provide and implement a central viewing process to analyze data (audit or data) from multiple components on the system. Related Control: AU-6(4) (Low/Mod/High) | CSA.ER-6.3(1) | N/A | AU-6(4) | x | x | x | CSF: ID.SC-4, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.3.2** Define an alternative or supplemental security mechanism on the CBRN device when the primary means of implemented security function is unavailable or compromised. Related Control: CP-13 (Low/Mod/High) | CSA.ER-6.3(2) | CS: EVR(10) | CP-13 | x | x | x | CSF: PR.PT-5 | | | |
| | | **6.3.3** Implement an incident handling capability for incidents consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery. Related Control: IR-4 (Low/Mod/High**)** | CSA.ER-6.3(3) | CS: EVR(2) | IR-4 | x | x | x | CSF: ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS-RP-1, RS.CO-3, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | | | | | | | | RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3 | | | |
| | | **6.3.4** Coordinate incident handling activities with contingency planning activities. Related Control: IR-4 (Low/Mod/High**)** | CSA.ER-6.3(4) | CS: EVR(2) | IR-4 | x | x | x | CSF: ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS-RP-1, RS.CO-3, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2 RC.CO-3 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.3.5** Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly. Related Control: IR-4 (Low/Mod/High**)** | CSA.ER-6.3(5) | CS: EVR(2) | IR-4 | x | x | x | CSF: ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS-RP-1, RS.CO-3, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2 RC.CO-3 | | | |
| | | **6.3.6** Ensure the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across | CSA.ER-6.3(6) | CS: EVR(2) | IR-4 | x | x | x | CSF: ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS-RP-1, RS.CO-3, RS.AN-1, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | the organization. Related Control: IR-4 (Low/Mod/High**)** | | | | | | | RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2 RC.CO-3 | | | |
| | | **6.3.7** Develop a risk response guide that can be used when findings from security assessments and monitoring are outside the threshold of CWMD's risk tolerance. Related Control: RA-7 Risk Response (Low/Mod/High) | CSA.ER-6.3(7) | CS: EVR(1), EVR(2), EVR(3), EVR(4), EVR(5), EVR(7), EVR(8), EVR(9), EVR(10), EVR(11) | RA-7 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | **6.4 Logging Capture & Trigger Support:** Generate, store, retain, delete, and report on specific CBRN device audit events, run specific audit checks, and report findings in a variety of ways. | **6.4.1** Ensure that audit records contain information that establish the following essential elements of event information: What type of event occurred; When the event occurred; Where the event occurred; Source of the event; Outcome of the event; and Identity of any individuals, subjects, or objects/entities associated with the event. Related Control: AU-2 (Low/Mod/High) | CSA.LCTS-6.4(1) | DI: AID(2) | AU-2 | x | x | x | CSF: PR.PT-1 | | | |
| | | **6.4.2** Capture audit record content that supports auditing functions, including event descriptions, time stamps, source | CSA.LCTS-6.4(2) | CS: LCT(1), RDL(1), RDL(2), RDL(5) | AU-3 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | and destination addresses, user or process identifiers, successful or failed indications, and filenames. Related Control: AU-3 (Low/Mod/High) | | | | | | | | | | |
| | **6.5 Support of Required Data Logging:** Capture required information in audit logs. | **6.5.1** Retain all CBRN device audit records consistent with the CWMD records retention policy for a (CWMD-defined time period) to support post-incident investigations that meet CWMD information retention requirements. Related Control: AU-11 (Low/Mod/High) | CSA.SRDL-6.5(1) | DI: AID(2) | AU-11 | x | x | x | CSF: PR.PT-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.5.2** Identify the types of events (e.g., password changes, failed logons or failed accesses related to systems, security or privacy attribute changes, administrative privilege usage, PIV credential usage, data action changes, query parameters, or external credential usage) that CBRN devices are capable of logging in support of auditing. Related Control: AU-2 (Low/Mod/High) | CSA.SRDL-6.5(2) | CS: LCT(1), RDL(1), RDL(2), RDL(5) | AU-2 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **6.5.3** Ensure that audit records contain information that establishes the following essential elements of event information:<br>a. What type of event occurred;<br>b. When the event occurred;<br>c. Where the event occurred;<br>d. Source of the event; Outcome of the event; and<br>e. Identity of any individuals, subjects, or objects/entities associated with the event.<br>Related Control: AU-3 (Low/Mod/High) | CSA.SRDL-6.5(3) | CS: RDL(6),CS:LSR(1) | AU-3 | x | x | x | CSF: PR.DS-4 | | | |
| | | **6.5.4** Implement audit log retention requirements and allocate supporting | CSA.SRDL-6.5(4) | CS: RDL(7), LSR(4) | AU-4 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | audit log storage capacities for CBRN devices. Related Control: AU-4 (Low/Mod/High) | | | | | | | | | | |
| | | **6.5.5** Alert within a (CWMD-defined time period) when allocated audit log storage volumes reach a (CWMD-defined percentage) of maximum audit log storage capacity. Related Control: AU-5(1) (High) | CSA.SRDL-6.5(5) | CS: RDL(7), AUP(5) | AU-5(1) | | | x | CSF: N/A | | | |
| | | **6.5.6** In the event of a primary audit logging failure, connect to an alternate audit logging capability that implements a minimum standard of auditing functionality determined by CWMD. Related Control: AU-5(5) | CSA.SRDL-6.5(6) | CS: AEI(2), RDL(3), LSR(2), LSR(3) | AU-5(5) | | | | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | **6.6 Support for Reliable Time:** Use timestamps to record the time an auditing event occurred. | **6.6.1** Generate time stamps of CBRN devices for audit records using internal system clocks. Related Control: AU-8 (Low/Mod/High) | CSA.SRT-6.6(1) | CS: SRT(1), SRT(3), SRT(4) | AU-8 | x | x | x | CSF: N/A | | | |
| | | **6.6.2** Record time stamps of CBRN devices for audit records that meet (CWMD-defined time measures) that implement local time offsets from Coordinated Universal Time (UTC). Related Control: AU-8 (Low/Mod/High) | CSA.SRT-6.6(2) | CS: SRT(1), SRT(3), SRT(4) | AU-8 | x | x | x | CSF: N/A | | | |
| | | **6.6.3** Synchronize CBRN device clocks within and between systems and components to compare internal system clocks at (CWMD-defined | CSA.SRT-6.6(3) | CS: SRT(1), SRT(3), SRT(4) | SC-45 | | | | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | frequencies) with UTC. Related Control: SC-45 | | | | | | | | | | |
| | | **6.6.4** Synchronize the internal system clocks to the UTC when the difference is greater than (CWMD-defined time period). Related Control: SC-45 | CSA.SRT-6.6(4) | CS: SRT(2) | SC-45 | | | | CSF: N/A | | | |
| | **6.7 Audit Support & Protection:** Support and protect audit activities and associated data for CBRN devices. | **6.7.1** Review and analyze CBRN device audit records for indications and potential impacts of inappropriate or unusual activity. Related Control: AU-5(5) | CSA.ASP-6.7(1) | CS: RDL(7), AUP(5) | AU-5(5) | | | | CSF: N/A | | | |
| | | **6.7.2** Implement audit record reduction and report generation capabilities that maintain original content and include | CSA.ASP-6.7(2) | CS: EVR(3), EVR(4), AUP(1), AUP(2), AUP(4) | AU-6 | x | x | x | CSF: ID.SC-4, DE.AE-2, DE.AE-3, DE.DP-4, RS.CO-2, RS.AN-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | modern data mining techniques to identify anomalous behavior in CBRN device audit records. Related Control: AU-6 (Low/Mod/High) | | | | | | | | | | |
| | | **6.7.3** Protect audit information and audit logging tools from unauthorized access, modification, and deletion. Related Control: AU-7 (Mod/High) | CSA.ASP-6.7(3) | CS: AUP(3) | AU-7 | | x | x | CSF: RS.AN-3 | | | |
| | | **6.7.4** Alert appropriate personnel upon detection of unauthorized access, modification, or deletion of audit information. Related Control: AU-9 (Low/Mod/High) | CSA.ASP-6.7(4) | CS: AUP(1), AUP(2), AUP(4), AUP(6), AUP(7) | AU-9 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | **6.8 State Awareness Support:** Differentiate between a device expected operation, from when it may be in a degraded cybersecurity state. | **6.8.1** Implement the security design principle of self-analysis in CBRN devices to assess the internal state of devices for data integrity and correct functionality in accordance with CWMD-established levels of trustworthiness. Related Control: SA-8(21) | CSA.SAS-6.8(1) | CS: AWR(1) | SA-8(21) | | | | CSF: PR.IP-2, ID.BE-5 | | | |
| | | **6.8.2** Verify the correct operation of security and privacy functions for CBRN devices in order to implement transitional states, alert appropriate personnel to failed security and privacy verification tests, and perform alternative | CSA.SAS-6.8(2) | CS: AWR(1) | SI-6 | | | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | actions (e.g., shut down device(s), restart device(s)) when anomalies are discovered. Related Control: SI-6 (High) | | | | | | | | | | |
| **7 Device Security:** *CWMD organizational requirements should be taken into consideration when determining CBRN cybersecurity at the device level, which can include technical features or functions implemented in the device's hardware and software.* | **7.1 Secure Execution:** CBRN devices MUST have the ability to respond to CWMD device level cybersecurity events. CWMD MUST have a policy that conforms CBRN devices to enable response features or functions that support event monitoring requirements. | **7.1.1** Separate user functionality that includes the user interface services from the system management functionality. Related Control: SC-2 (Mod/High) | DS.SE-7.1(1) | LA: ROL(4) DS: EXE(2), EXE(3) | SC-2 | | x | x | CSF: N/A | | | |
| | | **7.1.2** Maintain a separation of the executing processes for the device that includes but is not limited to logically separating CBRN software and firmware from other software, firmware, and data that be connected and limit | DS.SE-7.1(2) | DS: EXE(1), RSC(2), RSC(3), RSC(4) | SC-39 | x | x | x | CSF: N/A | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | access to potentially untrusted software to other system resources. Related Control:7.1.2 Maintain a separation of the executing processes for the device that includes but is not limited to logically separating CBRN software and firmware from other software, firmware, and data that be connected and limit access to potentially untrusted software to other system resources. Related Control: SC-39 (Low/Mod/High) | | | | | | | | | | |
| | **7.2 Secure Communication:** The CBRN device MUST have documentation | **7.2.1** Connect to external networks or other systems through a managed interface that consists | DS.SC-7.2(1) | CS: EIM(6) | SC-7 | x | x | x | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | that details how the device is expected to behave and how it establishes and/or terminates network connections. Also included should be the application of a secure mechanism for initiating or terminating communications. | of boundary protection devices (e.g., gateways, routers, firewalls, etc.) that adhere to CWMD security and privacy policies. Related Control: SC-7 (Low/Mod/High) | | | | | | | | | | |
| | | **7.2.2** Identify the protocol format for CBRN device uses and adhere to the protocol format to enable the detection of vulnerabilities or anomalies. Related Control: SC-7(17) | DS.SC-7.2(2) | DS: COM(2) | SC-7(17) | | | | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |
| | | **7.2.3** Protect data transmission that could include encryption techniques identified by CWMD policies. Related Control: SC-8 (Mod/High) | DS.SC-7.2(3) | DP: STX(2), STX(4) | SC-8 | | x | x | CSF: PR.DS-2 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **7.2.4** Terminate a network connection at the end of a communications session or a period of inactivity defined by CWMD policies. Related Control: SC-10 (Mod/High) | DS.SC-7.2(4) | DS: COM(3), COM(4), COM(5) | SC-10 | | x | x | CSF: N/A | | | |
| | | **7.2.5** Ensure that transmitted security and privacy attributes associated with the CBRN device information have not been modified in an unauthorized manner. Related Control: SC-16(2) | DS.SC-7.2(5) | DS: COM(11) | SC-16(2) | | | | CSF: DE.AE-1, | | | |
| | | **7.2.6** Verify the authenticity and integrity of data being received from other sources. Related Control: SC-21 (Low/Mod/High) | DS.SC-7.2(6) | DS: COM(8) | SC-21 | x | x | x | CSF: PR.PT-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | **7.2.7** Include resources for the protection of communications and the validity of transmitted information. Related Control: SC-23 (Mod/High) | DS.SC-7.2(7) | DS: COM(7), COM(9), COM(10) | SC-23 | | x | x | CSF: PR.PT-4 | | | |
| | | **7.2.8** Include protections for hardware-based write protection that cannot be disabled without proper permission. Related Control: SC-51 | DS.SC-7.2(8) | DS: COM(3), RSC(9) | SC-51 | | | | CSF: N/A | | | |
| | **7.3 Secure Resource Usage in a Degraded State:** The CBRN device MUST have the ability to function in a degraded state to ensure that any information is | **7.3.1** Enter a safe mode of operation when abnormal behaviors are detected or observed with a CBRN device with limited network access until, at a predetermined time defined by CWMD, | DS.SRUD-7.3(1) | DS: RSC(6), OPS(3), OPS(4), OPS(6) | CP-12 | | | | CSF: PR.PT-5 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | not lost, or it should have the capability to be shut down and taken off the network until the device has been restored to a known good state. | the device can be deemed safe for normal use. Related Control: CP-12 | | | | | | | | | | |
| | | **7.3.2** Prevent the unauthorized or unintended transfer of information from shared resources. This includes encrypted information transfers from CBRN devices. Related Control: SC-4 (Mod/High) | DS.SRUD-7.3(2) | DS: RSC(1) | SC-4 | | x | x | CSF: N/A | | | |
| | | **7.3.3** If applicable, include protections that can filter certain types of packets to protect system components on internal networks from being affected by or source of denial-of-service attacks. Related | DS.SRUD-7.3(3) | DS: RSC(5), RSC(8) | SC-5 | x | x | x | CSF: PR.DS-4, DE.CM-1, PR.PT-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | Control: SC-5 (Low/Mod/High) | | | | | | | | | | |
| | | **7.3.4** The CBRN device should fail to a known state defined by CWMD while preserving data confidentiality, integrity, and availability of the device if such a failure occurs. CWMD should define the system failures and outline processes and procedures for the restoration of the device. Related Control: SC-24 (High) | DS.SRUD-7.3(4) | DS: RSC(6), OPS(3), OPS(5), OPS(6), OPS(8) | SC-24 | | | x | CSF: N/A | | | |
| | | **7.3.5** The CBRN device should have reliable hardware protection against reprogramming the memory, from the | DS.SRUD-7.3(5) | DS: RSC(7), DIN(5) | SC-34 | | | | CSF: PR.PT-4 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | point of the initial writing to the insertion of the memory into the CBRN device. Related Control: SC-34 | | | | | | | | | | |
| | | **7.3.6** Outline the fail-safe procedures the user can follow if an indicated failure occurs with the CBRN device. Related Control: SI-17 | DS.SRUD-7.3(6) | DS: RSC(6) | SI-17 | | | | CSF: N/A | | | |
| | **7.4 Device Integrity:** Enforce protection mechanisms against unauthorized changes to the hardware or software of CBRN devices. | **7.4.1** Perform security and privacy checks on the CBRN device prior to the establishment of network connections. Related Control: CA-9(1) | DS.DI-7.4(1) | DP: DS: DIN(1) | CA-9(1) | | | | CSF: ID.AM-3 | | | |
| | | **7.4.2** Employment of anti-tamper technologies, tools, and techniques should be applied throughout the | DS.DI-7.4(2) | DS: DIN(3) | SR-9(1) | | | x | CSF: DE.DP-2 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | system development lifecycle. Related Control: SR-9(1) (High) | | | | | | | | | | |
| | **7.5 Secure Network Onboarding Support:** Use secure network onboarding technologies to support the secure network onboarding of CBRN devices. | **7.5.1** Employ password authentication mechanisms that include: A list of commonly used, expected, or compromised passwords and the list should be updated periodically. a. When users of the CBRN device create or update passwords, the passwords are not found on the commonly used, expected, or compromised passwords list. b. All passwords should be cryptographically protected on all CBRN | DS.SNOS-7.5(1) | DS: ONB(2), ONB(3) | IA-5(1) | x | x | x | CSF: PR.AC-1, PR.AC-6, PR.AC-7 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | devices. Related Control: IA-5(1) (Low/Mod/High) | | | | | | | | | | |
| | | **7.5.2** The CRBN device should only connect to external networks or other systems through a managed interface that consists of boundary protection devices (e.g., gateways, routers, firewalls, etc.) that adhere to CWMD security and privacy policies. Related Control: SC-7 (Low/Mod/High) | DS.SNOS-7.5(2) | CS: EIM(6) | SC-7 | x | x | x | CSF: PR.AC-5, PR.DS-5, PR.PT-4, DE.CM-1 | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | **7.6 Secure Device Operation:** Employ internal and external safeguards for the secured use of CBRN devices in various operational states. | **7.6.1** The CBRN device should recover and reconstitute to a known good state within a period of time defined by CWMD policies and procedures after a disruption, compromise, or failure of the CBRN device. Related Control: CP-10 (Low/Mod/High) | DS.SDO-7.6(1) | DP: OPS(3) | CP-10 | x | x | x | CSF: RS.RP-1, RC.RP-1, PR.IP-9 | | | |
| | | **7.6.2** The CBRN device should automatically disable the system if security violations are detected (e.g., cyber-attack, exfiltration of device information, errors in the programming software, etc.). Related Control: IR-4(5) | DS.SDO-7.6(2) | DS: OPS(7) | IR-4(5) | | | | CSF: ID.SC-5, DE.AE-2, DE.AE-3, DE.AE-4, DE.AE-5, RS-RP-1, RS.CO-3, RS.AN-1, RS.AN-2, RS.AN-3, RS.AN-4, RS.MI-1, RS.MI-2, RS.IM-1, | | | |

| CWMD Cyber Security Best Practices | | | CWMD Best Practice Identifier | NIST SP 800-213A Technical Capabilities | NIST SP 800-53r5 | FIPS 199 Security Impact Levels | | | NIST Cybersecurity Framework | CWMD Implementation Benchmarks | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Capabilities | Sub-capabilities | Best Practice | ID | Technical Capabilities | Security Control | Low | Mod | High | NIST Informative References | Fully Implemented | Partially Implemented | Not Implemented |
| | | | | | | | | | RS.IM-2, RC.RP-1, RC.IM-1, RC.IM-2, RC.CO-1, RC.CO-2, RC.CO-3 | | | |

# Appendix D – Federal Guidelines

This is a list of U.S. Federal cybersecurity guidance to be considered before planning Test and Evaluation (T&E) approaches.

DHS Sensitive Systems Policy Directive 4300A Version 13.1

DHS 4300A, Sensitive Systems Handbook

DHS CWMD Acquisition Division Policy Memo

DHS CWMD T&E 500 CWMD 123660 Version 2

DHS Directive 026-06, Test and Evaluation

DHS OCISO Small Unmanned Aircraft System

DHS S&T Cyber Resilience T&E Guide Version 2

DHS S&T Cybersecurity Acquisition Lifecycle

DHS S&T Cybersecurity Systems Engineering

DHS System Security Authorization Process

DHS Threat Assessment Support of T&E

NISTIR 8228, Considerations for Managing Internet of things (IoT) Cyber security and Privacy Risks

NISTIR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers

NISTIR 8259A, IoT Device Cybersecurity Capability Core Baseline

NISTIR 8286, Integrating Cybersecurity and Enterprise Risk Management (ERM)

NIST-SP 800-160, Developing Cyber-Resilient Systems: A Systems Security Engineering Approach, Volume 2, Revision 1

NIST-SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems, Volume 1

NIST-SP 800-161, Supply Chain Risk Management Practices for Federal Information Systems and Organizations

NIST-SP 800-163, Vetting the Security of Mobile Applications, Revision 1

NIST-SP 800-30, Guide for Conducting Risk Assessments, Revision 1

NIST-SP 800-37r2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy

NIST-SP 800-53Ar5, Assessing Security and Privacy Controls in Information Systems and Organizations

NIST-SP 800-53R5, Security and Privacy Controls for Information Systems and Organizations

NIST-SP 53Br5, Control Baselines for Information Systems and Organizations

NIST-SP 800-60v1r1, Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories

NIST-SP 800-60v2r1, Guide for Mapping Types of Information and Information Systems to Security Categories

NIST-SP 800-82r2, Guide to Industrial Control Systems (ICS) Security

NIST-SP 800-213A, IoT Device Cybersecurity Guidance for the Federal Government: IoT Device Cybersecurity Requirement Catalog

# Pacific Northwest National Laboratory

902 Battelle Boulevard
P.O. Box 999
Richland, WA 99354

1-888-375-PNNL (7665)

***www.pnnl.gov***