Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure

Issued by the Office of the National Cyber Director, following consultation with the Cybersecurity and Infrastructure Security Agency

December 13, 2024

Ver 1.0

Preface

Among the most significant and growing issues facing our Nation is that of cybersecurity threats to our critical infrastructure. The degradation, destruction, or malfunction of these systems that control and operate the critical infrastructure could cause significant harm to the national and economic security of the United States.

The responsibility to secure and manage the nation's critical infrastructure is shared among a number of parties, including owners and operators; the Federal Government; and State, local, Tribal, and territorial (SLTT) governments.

It is the policy of the United States to safeguard the critical infrastructure of the Nation with a particular focus on the cybersecurity and resilience of systems supporting National Critical Functions[1]—functions of Government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on national security, economic security, public health or safety, or any combination thereof.[2]

Given the importance of securing Nation's critical infrastructure, the Government has made a historic investment through the passage of the Infrastructure Investment and Jobs Act (IIJA), Inflation Reduction Act (IRA), and Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act. The United States has a unique opportunity and national security imperative to build cyber resilience into this next generation of American infrastructure.

Further, the National Cybersecurity Strategy recognizes that "Federal grant programs offer strategic opportunities to make investments in critical infrastructure that are designed, developed, fielded, and maintained with cybersecurity and all-hazards resilience in mind."[3] Additionally, in the National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (NSM-22), the President established an objective to "[l]everage Federal Government agreements, including grants, loans, and procurement processes, to require or encourage owners and operators to meet or exceed minimum security and resilience requirements."[4]

NSM-22 further provides that "[w]here applicable law limits the ability of Federal departments and agencies to establish minimum requirements through agreements, they shall provide

---

[1] *See* National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/; *see also* CISA: National Critical Functions, https://www.cisa.gov/topics/risk-management/national-critical-functions.

[2] *See* National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

[3] The White House, "National Cybersecurity Strategy," March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

[4] *See* National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

guidance and recommendations for appropriate security and resilience measures alongside the provision of Federal funding."

Therefore, all grant-making agencies are encouraged to incorporate cybersecurity requirements into their respective grant programs for critical infrastructure. Federal agencies can do so by including cybersecurity requirements language in Notice of Funding Opportunities (NOFOs) and Terms and Conditions (T&Cs) to ensure grant recipients develop and maintain Project Cyber Risk Assessments and Project Cybersecurity Plans for these projects.

The guidance provided in this document (herein referred to as "Playbook") does not waive or replace any other cybersecurity requirements that may apply to critical infrastructure or other types of grant projects.

This Playbook is intended to assist managers of relevant Federal grant programs and grant recipients; however, all Federal financial assistance programs can benefit from taking a similar approach to analyze their lifecycle activities and identify opportunities for strengthening the cybersecurity of critical infrastructure. Agencies should consider establishing cost thresholds or other criteria for applying this Playbook to specific projects.

This Playbook is advisory in nature. It has no direct effect on any Federal grant program or recipient. It is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

This Playbook provides recommended requirements, model language, resources, and guidance for strengthening cybersecurity in Federal grant programs for critical infrastructure. This Playbook will be periodically reviewed and updated, as required.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Purpose

The purpose of this Playbook is to provide an easy-to-use resource for Federal agencies and grant recipients to strengthen cybersecurity in critical infrastructure projects. The Playbook provides guidance for projects that include technologies that, if impacted by a cyber incident, could affect the safety, reliability, or operability of critical infrastructure.

Critical infrastructure owners and operators must be vigilant against growing risks posed by inadequately secured systems and should take measures to strengthen and secure systems to maintain safe, functional, and resilient critical infrastructure. Our nation's critical infrastructure is at risk, in part, because legacy systems, built without the forethought of cybersecurity, are largely still in use.

The Infrastructure Investment and Jobs Act (IIJA), Inflation Reduction Act (IRA), and Creating Helpful Incentives to Produce Semiconductors (CHIPS) and Science Act provide historic investments in the nation's critical infrastructure and provide an opportunity to ensure we build and maintain infrastructure that is resilient to cyber threats and aligned with the secure and resilient-by-design principles set forth in the National Cybersecurity Strategy and NSM-22.[5]

The Office of the National Cyber Director (ONCD) issues this Playbook resource in furtherance of the strategic objectives in the National Cybersecurity Strategy. The Cybersecurity and Infrastructure Security Agency (CISA) and other departments and agencies provided technical expertise in the development of this Playbook. This Playbook is intended to provide Federal agencies and grant recipients with tools to build cyber resilience into their projects. Adding cybersecurity requirements into Federal funding programs and upholding them throughout the projects' lifecycle allows grant program managers, recipients, and subrecipients to identify, prioritize, and address key cyber risks more easily. Safeguarding the future of American infrastructure requires collaboration between the Federal Government; SLTT governments; and critical infrastructure owners and operators.

Federal agencies should include provisions such as cybersecurity principles, best practices, and controls in their awards and subawards, consistent with applicable law and guidance. The recommended cybersecurity requirements in this Playbook help recipients develop long-term strategies to continuously address cyber risk on asset performance. Where appropriate, agencies should encourage recipients and subrecipients to set cybersecurity goals above the baseline requirements. A Project Cyber Risk Assessment and Project Cybersecurity Plan, as outlined in Section 3, should be required for every critical infrastructure grant project that has a technology nexus.

In instances where a recipient has multiple projects within a system, it may be appropriate to develop an overall plan for the system. These systems and assets may include elements, components, and full systems of information technology (IT), operational technology (OT),

[5] The White House, "National Cybersecurity Strategy," March 2023, https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf.

industrial control systems (ICS), supervisory control and data acquisition (SCADA), and other systems.

1.2 Playbook Overview

The *Playbook for Strengthening Cybersecurity in Federal Grant Programs for Critical Infrastructure* (Playbook) is intended to strengthen cybersecurity in critical infrastructure projects. The Playbook provides model language for requirements for grant-awarding agencies to use in notices, and terms and conditions to require and provide resources and tools for grant recipients and subrecipients.

Federal grant-awarding agencies[6] should consider whether the programs they administer will fund projects that incorporate technology likely to present cyber risk to critical infrastructure. For projects that incorporate such technology, Federal grant-awarding agencies, as appropriate and consistent with applicable law, or when regulations or directives do not already require similar actions, should apply the elements and recommendations in this Playbook. The guidance in this Playbook is not intended to conflict with other grant cybersecurity guidance provided by an agency, but rather is to serve as a complementary resource for agencies and recipients.

In cases where a Federal agency provides funding to a recipient, such as a State Government or others that may serve as a Pass-Through Entity (PTE),[7] the PTE should apply this guidance to subawards.

The Playbook contains:

- **Recommended cybersecurity actions and best practices** for Federal grant agencies, recipients, and subrecipients to incorporate into the grants management lifecycle.
- **Model language for cybersecurity requirements** for inclusion in Notices of Funding Opportunities (NOFOs) or other grant program guidance and announcements.
- **Model language for grant award terms and conditions (T&Cs).**
- **A template and tools for developing a Project Cyber Risk Assessment**.
- **A template for developing a Project Cybersecurity Plan.**
- **Resources that outline cybersecurity best practices** that program managers and recipients can use to create, clarify, or communicate programmatic cybersecurity requirements.

1.3 How to Use this Playbook

This Playbook provides cyber risk mitigation resources, tools, and references for Federal agencies, grant program managers, pass-through entities, such as State governments, and recipients.

---

[6] https://www.grants.gov/learn-grants/grant-making-agencies.html

[7] *See* 2 C.F.R. § 200.1 ("Pass-through entity (PTE) means a non-Federal entity that provides a subaward to a subrecipient to carry out part of a Federal program.").

Federal agencies and grant program leaders and managers should:

- Review Sections 4 and 5 for recommended actions to incorporate and oversee cybersecurity requirements throughout the grant management process in grant programs for critical infrastructure and determine steps for program-specific implementation.
- Review Section 5 for model cybersecurity requirements language in NOFOs, and award Terms and Conditions (T&Cs).

Grant recipients should:

- Review section 3 (Project Cyber Risk Assessments and Project Cybersecurity Plan).
- Review section 6 (Grant Recipient Resources).
- Review and use, as appropriate, Appendix C (CISA CPG Checklist Adapted for Grant Recipients).
- Review and use, as appropriate, Appendix D (Project Cyber Risk Assessment and Project Cybersecurity Plan Sample Templates).
- Review and use, as appropriate, Appendix E (Cybersecurity Resources for Grant Recipient Project Execution).

2 Cybersecurity and Grant Management Overview

2.1 Overview of Critical Infrastructure Cybersecurity Guidelines

The term critical infrastructure is defined as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."[8]

The critical infrastructure community includes public and private owners and operators and government entities with a role in enhancing the security and resilience of the nation's infrastructure. Advances in technology have resulted in increased efficiency and automation in many regards, but also have introduced new risks. Many critical infrastructure functions are performed or supported by a broad category of technologies, including information technology (IT), operational technology (OT), industrial control system (ICS), cyber-physical systems (CPS), and connected devices—to include internet of things (IOT) and industrial internet of things (IIOT) devices.

The National Institute of Standards and Technology (NIST) develops cybersecurity standards, guidelines, and best practices for U.S. industry, Federal agencies, and the broader public. NIST developed *The Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity

[8] Critical Infrastructures Protection Act of 2001, Pub. L. No. 107-56, Title X, § 1016 (codified at 42 U.S.C. § 5195c(e)).

Framework), a framework to reduce cyber risks to critical infrastructure, which assists owners and operators of critical infrastructure to identify, assess, and manage cyber risks.[9,10]

In 2021, President Biden issued the *National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems (NSM-5)*.[11] This memorandum directed the Cybersecurity and Infrastructure Security Agency (CISA), in coordination with NIST and other Federal agencies, to develop voluntary cross-sector Cybersecurity Performance Goals (CPGs), which are a prioritized subset of IT and OT cybersecurity best practices aimed at meaningfully reducing risks to both critical infrastructure operations and to the American people.[12] These CPGs are applicable across all critical infrastructure sectors, align with the NIST Cybersecurity Framework, and establish the baseline cybersecurity best practices and controls that grant program managers (PMs) should require, to the extent consistent with law and applicable guidance. Some critical infrastructure sectors have tailored these CPGs for entities in their sector. Grant recipients and subrecipients should plan to implement CPGs as part of their project lifecycle, where appropriate.

As noted above, NSM-22[13] established an objective to leverage Federal Government agreements, including grants, loans, and procurement processes to require or encourage critical infrastructure owners and operators to meet or exceed minimum security and resilience requirements.

Additionally, the Office of Management and Budget (OMB) revised the OMB Guidance for Grants and Agreements, now called the "OMB Guidance for Federal Financial Assistance."[14] The effective date for the guidance was October 1, 2024. These revisions provide clarity and updated guidance to Federal agencies regarding the consistent and efficient use of Federal financial assistance. In the guidance, OMB added a requirement in paragraph (e) of section 200.303 that recipient and subrecipient internal controls include cybersecurity and other measures to safeguard information. This Playbook is meant to complement OMB's guidance in section 200.303.

2.2 Introduction to Grants Management Business Standards

This section provides background for grant program managers to further understand how to incorporate cybersecurity principles and controls into the grant management lifecycle.

---

[9] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," https://www.nist.gov/cyberframework.

[10] This document references the CISA CPGs and the NIST Cybersecurity Framework (CSF) – upon which the CPGs are based. On February 26th, 2024, NIST published CSF 2.0. Subsequent versions of this Playbook may be updated as additional guidance is released related to updated CPGs and other resources related to the CSF 2.0 release.

[11] National Security Memorandum on Improving Cybersecurity for Critical Infrastructure Control Systems, July 28, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/07/28/national-security-memorandum-on-improving-cybersecurity-for-critical-infrastructure-control-systems/.

[12] CISA, "Cross-Sector Cybersecurity Performance Goals Report," September 2, 2022, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

[13] *See* National Security Memorandum on Critical Infrastructure Security and Resilience (NSM-22), April 30, 2024, https://www.whitehouse.gov/briefing-room/presidential-actions/2024/04/30/national-security-memorandum-on-critical-infrastructure-security-and-resilience/.

[14] https://www.federalregister.gov/documents/2024/04/22/2024-07496/guidance-for-federal-financial-assistance

The Federal Government has documented the business standards for Federal grants management using the Federal Integrated Business Framework (FIBF).[15] These FIBF grants Management Business Standards were developed by a cross-agency working group and approved by the Office of Management and Budget (OMB).[16]

The Federal Grants Management Business Lifecycle, depicted in Figure 1, is a component of the FIBF Grants Management Business Standards and is segmented into functions and activities to categorize and describe the business processes and subprocesses of Federal grants management. Grant program level activities include those necessary for a grantmaking entity to manage its grant program. Grant project level activities include those that a grantmaking entity performs to manage grant recipient projects funded in whole or in part by the grantmaking entity's program.

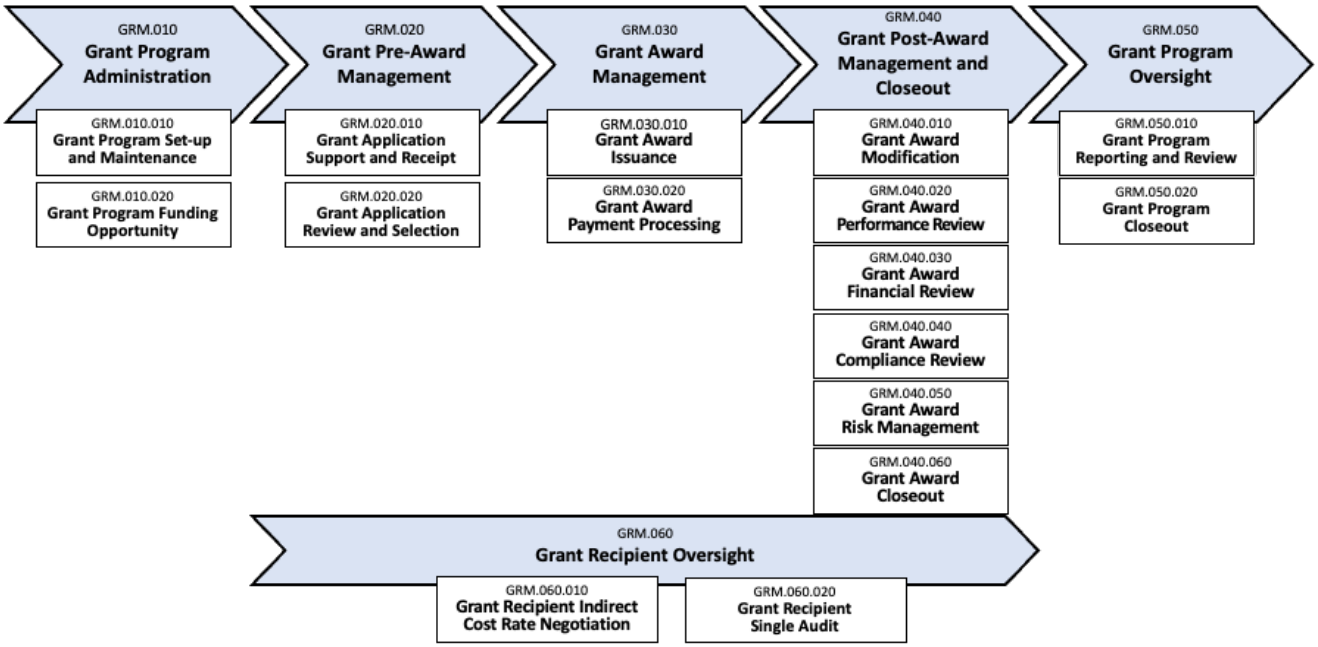

Figure 1: Federal Grants Management Business Lifecycle

As documented, the FIBF Grants Management functions and activities reflect the common business processes of Federal grant programs; however, this standard set of functions and activities is also representative of the activities performed by grant recipients who issue subawards to subrecipients. Additionally, the Federal Grants Management Business Lifecycle documents the common business processes for Federal and PTE management of both discretionary and non-discretionary grant programs.

[15] General Services Administration Office of Shared Solutions and Performance Improvement (GSA OSSPI), "Federal Integrated Business Framework," https://ussm.gsa.gov/fibf/.

[16] GSA OSSPI, "Federal Integrated Business Framework – Grants Management," https://ussm.gsa.gov/fibf-gm/.

3 Project Cyber Risk Assessments and Project Cybersecurity Plans

Actions taken to mitigate the cyber risk to critical infrastructure are more effective when executed throughout the full lifecycle of projects, beginning with the principles of Secure by Design.[17] Incorporating Secure by Design principles into technology and project design and development is one of the most effective steps technology manufacturers can take to mitigate cyber risk. Additionally, all grant recipients are encouraged to take advantage of no-cost services provided by CISA[18] and other government agencies. Finally, performing a Project Cyber Risk Assessment and developing and implementing a Project Cybersecurity Plan for grant projects is a key element in enhancing critical infrastructure cybersecurity.

Conducting a Project Cyber Risk Assessment is essential to understanding the potential physical impact resulting from an incident or occurrence to IT, OT, ICS, and other systems essential to the safe and reliable operation of facilities, systems, and equipment. Conducting a Project Cyber Risk Assessment reveals potential vulnerabilities and their potential impact to improve the overall safety and resiliency and cyber posture necessary to meet operational and mission needs. By conducting such assessments, organizations can establish an appropriate baseline of cybersecurity actions then develop a Project Cybersecurity Plan.

Recipients and subrecipients should conduct a Project Cyber Risk Assessment and develop a Project Cybersecurity Plan during the project design phase. PMs will need to determine the appropriate timeframe for the attestation or submission of the assessment and plan based on the scope and complexity of the project and its lifecycle.

The Project Cyber Risk Assessment and Project Cybersecurity Plan will assist recipients in implementing baseline cybersecurity best practices and controls as part of the execution of the grant award, reduce project cybersecurity risk, and reduce the risk of disruption to critical infrastructure.

3.1 The Project Cyber Risk Assessment

The *CISA CPG Checklist Adapted for Grant Recipients* (*Cyber Risk Assessment Tool*), provided in Appendix C, is available to recipients for performing assessments of project cyber risks and applying mitigation best practices and controls. This checklist is modeled after CISA's *Cross-Sector CPG Checklist* and includes modifications to enable grant recipients to assess cybersecurity best practices and controls for both the project and the recipient's organization.

- Assessments at the project level include an assessment of any project IT/OT assets that are designed, developed, operated, or maintained as part of the execution of the project.
- Assessments at the organizational level include assessing the recipient organization's overall cyber risk posture.

[17] CISA: Secure by Design, https://www.cisa.gov/securebydesign.

[18] CISA: Free Cybersecurity Services and Tools, https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools.

Grant recipients may use the CISA Cybersecurity Performance Goal (CPG) Checklist Adapted for Grant Awards (Risk Assessment Tool) or use another assessment tool that meets or exceeds all CPG categories.

Due to varying degrees of project complexity, each item included in the Appendix C checklist may not be applicable to every project. Recipients should review and consider each item and apply risk mitigations, as appropriate.

Recipients are encouraged, but not required, to assess and address the cybersecurity of their organization. Improving the cybersecurity posture of an organization reduces vulnerabilities of project IT/OT cyber assets, protects against lateral movement attacks, and further reduces grant award project risk.

3.2 The Project Cybersecurity Plan

Developing a project cybersecurity plan is critical for managing risk, securing systems, and protecting against growing cyber threats. Appendix D contains a *Project Cybersecurity Plan* template that may be used by grant recipients when developing and maintaining their Project Cybersecurity Plans. This template may be useful to identify and mitigate gaps in cybersecurity practices and controls.

Note: A companion Microsoft Excel fillable worksheet is available.

The Project Cybersecurity Plan should include:

(A) Identifying grant award information.
(B) A high-level description of the plan for the overall management of the project's cybersecurity program, including a high-level description of how resources, roles, and responsibilities will be managed.
(C) An inventory of project IT/OT technology assets.
(D) A list of planned cybersecurity risk mitigation actions and controls, including:
  i. A prioritized list of assessment gaps that need to be addressed; and
  ii. A list of cybersecurity risk mitigation actions to be undertaken as part of execution of the grant award, with a target implementation date identified for each mitigation.

3.3 The Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update

The Cybersecurity Plan Annual Update should include information from the initial or previous plan and include, at a minimum:

Section C: An updated inventory of project IT/OT technology assets.
Section E: An updated list of planned cybersecurity actions with modifications, if any, including:

(i) An updated prioritized list of project cybersecurity gaps;
(ii) The list of planned cybersecurity actions with modifications, if any; and

(iii) The current status of the cybersecurity risk mitigation actions; with an updated implementation date for each mitigation.

The Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update must contain sufficient information to demonstrate the recipient has taken appropriate actions to mitigate cybersecurity risks.

The *Project Cyber Risk Assessment and Project Cybersecurity Plan* template in Appendix C & D, and the companion Excel spreadsheet, are designed to facilitate the assessment and plan and Annual Update. An updated assessment and plan should be required on an annual basis while the grant remains open.

3.4 Project Cyber Risk Assessment and Project Cybersecurity Plan Closeout

The Closeout Project Cyber Risk Assessment and Project Cybersecurity Plan should include all information required in the Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update along with disposition instructions and system documentation for transfer of critical infrastructure cyber asset(s) (IT/OT assets).

For grant awards that include equipment or property whose ownership may be transferred, the Federal awarding agency should include grant agreement provisions to ensure transfer of information pertaining to cyber asset design, operation, and necessary cybersecurity best practices and controls.

The Closeout should provide disposition instructions and system documentation (e.g., cyber risk assessment, cybersecurity plan, any system manuals or guides, system specifications) for the transference of critical infrastructure cyber asset(s) to the new owner/operator.

3.5 Agency Determination of Attestation or Submission of Assessments and Plans.

Awarding entities should determine the type and level of appropriate compliance monitoring for projects based on several considerations. Consideration factors may include, but not be limited to:

- Projects associated with known threats, hazards, and vulnerabilities;
- Projects with long lifespans; and
- Projects that are so critical or highly technology-centric that the risk of a malicious or accidental cyber incident may result in a significant impact or consequences for public health or safety, economic security, or national security.

If a recipient fails to comply with cybersecurity Terms and Conditions, the grant agency may take one or more actions consistent with agency procedures and policies, such as placing the recipient on a corrective action plan, withholding further awards, or wholly or partly suspend the grant pending corrective action.

4 Recommendations for Federal Awarding Agencies Issuing Grants, including Pass Through Entities (PTEs).

Cybersecurity should be integrated into activities performed by grant making agencies and recipients throughout the program management lifecycle of the project. The following actions, consistent with applicable law, regulations, and OMB guidance, can reduce programmatic risk and enable recipients to effectively manage and communicate cybersecurity risk for their funded projects. These actions are designed to assist awarding agencies and recipients in achieving the objectives of their award projects. While the cybersecurity actions in this Playbook are meant to serve as guidance across all federal critical infrastructure grant programs, agencies may tailor them to fit their processes, as appropriate.

In cases where Federal grants are provided to a recipient which serves as a PTE that provides subawards, the PTE has responsibility for ensuring the subrecipient develops and maintains a Project Cyber Risk Assessment and Project Cybersecurity Plan, as necessary. Agencies should include the following requirements in the terms and conditions for all critical infrastructure grants with a technology nexus:

- A Project Cyber Risk Assessment;
- A Project Cybersecurity Plan; and
- A requirement for either: (a) attestation to having developed a Project Cyber Risk Assessment and a Project Cybersecurity Plan, or (b) submission and acceptance of the assessment and plan by the grantmaking agency's program manager.

Note: If the Federal agency possesses a copy of the Project Cyber Risk Assessment and Project Cybersecurity Plan, it must appropriately mark, maintain and protect the materials from disclosure, as permitted by law. If disclosed, assessment and plan information may allow malicious actors to exploit documented critical infrastructure vulnerabilities.

Federal grant awarding agencies should advise recipients to specifically identify in their plans whether they seek protection from disclosure of any sensitive content through marking that specific content in the plan (e.g., segregate sensitive content into a separate annex for ease of identification) and explaining the nature of the sensitivities, consistent with Data Protection laws. Federal agencies may also identify information it may protect from disclosure under a Freedom of Information Act (FOIA) request through marking applicable release exemptions accordingly, to the extent possible.

Some Project Cyber Risk Assessments and Project Cybersecurity Plans may be eligible for protection under the CISA Protected Critical Infrastructure Information (PCII) Program.[19] Federal awarding agencies may contact the CISA PCII Program Office for further information on how these protections might be extended to grantees.

[19] Please visit CISA's website for more information about the PCII Program at https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program.

Table 1: Recommended Actions for Grant Awards

Index	Activity[20]	Grant Program Action (Federal and PTE)	Grant Award Recipient Action
1	Grant Program Set-up and Maintenance	Identify critical infrastructure grant programs and types of projects that include a technology nexus that may pose a cyber risk that would affect the reliability or operability of critical infrastructure.	(N/A)
2	Grant Program Funding Opportunity	Issue NOFO or other grant program guidance or announcements with post-award requirements for Project Cyber Risk Assessments and Project Cybersecurity Plans. (Refer to Section 5 for model NOFO and grant award T&C language). Determine the appropriate timeframe for the completion of a Project Cyber Risk Assessment and the development of a Project Cybersecurity Plan. The due date for development should be determined based on the scope and complexity of the project; however, the plan should be developed no later than during the design phase of the project.	(N/A)
3	Grant Application Support	As appropriate, provide potential grant applicant community information on post-award Project Cyber Risk Assessment and Project Cybersecurity Plan requirements and available assistance through grant program resources (Reference Appendices C, D, and E for guidance).	If needed, request additional information about post-award Project Cyber Risk Assessment and Project Cybersecurity Plan requirements and available assistance.
4	Grant Application Review and Selection	Identify selected critical infrastructure projects that include a technology nexus that may pose a cyber risk that would affect the reliability or operability of critical infrastructure, and request additional proposed project information, as needed.[21]	If requested, provide additional proposed project information

[20] These activities are based on the Grant Risk Management lifecycle.

[21] Identifying projects with critical cyber assets during the application review and selection activity is not intended to suggest that the existence of critical cyber assets should be a contributing factor to application selection. This action is intended to expedite the identification and prioritization of projects warranting a Project Cyber Risk Assessment and Project Cybersecurity Plan during the grant award issuance activity.

Index	Activity[20]	Grant Program Action (Federal and PTE)	Grant Award Recipient Action
5	Grant Award Issuance	As appropriate, coordinate with the selected award recipient details about the Project Cyber Risk Assessment and Project Cybersecurity Plan, including attestation requirements or requirements for submission of the assessment and plan, associated timeframe submission requirements, any specific controls, activities, or best practices that should be included in the plan or risk to be mitigated, how the plan will be protected, and how implementation of the plan may be verified, if necessary. Execute grant award with agreed upon T&Cs and request follow-on annual updates during the project lifecycle.[22] Provide technical assistance, if available, or resources for completing a Project Cyber Risk Assessments and developing a Project Cybersecurity Plan to the grant recipient (see Appendices C, D, E). Receive attestation to or submission of the recipient's assessment and plan within the specified timeframe.[23] If a submission of the assessment and plan is directed by the agency, evaluate, and notify grant recipient of Plan approval, or document and provide recommendations for remediation and adoption.	Develop and attest to (or submit, if required) a Project Cyber Risk Assessment and Project Cybersecurity Plan within the specified time of award issuance. Maintain and update the Plan during the project lifecycle.
6	Grant Award Payment Processing	If the Project Cyber Risk Assessment and Project Cybersecurity Plan are not attested to or submitted within the specified timeframe as required in the grant agreement and T&Cs, agencies should utilize their grant oversight provisions and apply applicable enforcement provisions to obtain required items	Before submitting a request for subsequent payment, ensure a Project Cyber Risk Assessment and Project Cybersecurity Plan is developed and attested to, or submitted and approved, if required. If changes to a Project

[22] Timelines for this table are illustrative and may be adjusted to account for the specifics of the program, specifically, a Project Cyber Risk Assessment and Project Cybersecurity Plan should be developed and approved during the project design phase.

[23] Grant PMs should put in place policies and procedures to protect grant recipient assessments and plans. If exposed, cybersecurity assessment and plan information may allow malicious actors to exploit documented critical infrastructure vulnerabilities. Federal awarding agencies should advise recipients to specifically identify in their plans whether they seek protection from disclosure of any sensitive content, mark that specific content in the plan (possibly by segregating it into a separate annex for ease of identifying), and explain the nature of those sensitivities. This will allow Federal agencies to protect the information in the event of a Freedom of Information Act (FOIA) request.

Index	Activity[20]	Grant Program Action (Federal and PTE)	Grant Award Recipient Action
			Cyber Risk Assessment and Project Cybersecurity Plan have been made, ensure that the changes have been submitted and accepted, if required.
7	Grant Award Performance Review	Ensure grant recipient develops and attests to, or submits, if required, a Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update, as well as associated recommendations, updates, and concerns, if any. Provide assistance, as available, in identifying best practices or acceptable alternative actions to address Project Cyber Risk Assessment and Project Cybersecurity Plan concerns.	Update the Project Cyber Risk Assessment and Project Cybersecurity Plan annually during the period of performance, and attest to or submit, as required. If issues and concerns are identified, request additional information, technical assistance, and identify actions needed to address cybersecurity issues and concerns. If a modification to the Project Cybersecurity Plan is needed, prepare the modification.
8	Grant Award Compliance Review	Determine if the Project Cyber Risk Assessment and Project Cybersecurity Plan were submitted or attested to within the specified timeframe. Determine if Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Updates were submitted annually during the duration of the grant.	None.

Index	Activity[20]	Grant Program Action (Federal and PTE)	Grant Award Recipient Action
9	Grant Award Risk Management	If the Grants Program Manager becomes aware of evidence that the award recipient has not followed or updated their Project Cyber Risk Assessment and Project Cybersecurity Plan, consider actions necessary to verify that the recipient is in compliance with all agreed upon T&Cs. If the Grant Program Manager becomes aware that the recipients' cybersecurity assessment and plan does not address new or emergent risks that are critical to the program, consider updating the award to include new T&Cs to address the risks.	Annually review and update the Project Cyber Risk Assessment and Project Cybersecurity Plan.
10	Grant Award Closeout	Review closeout Project Cyber Risk Assessment and Project Cybersecurity Plan parameters and execute as appropriate, per the grant award T&Cs.	Submit closeout Project Cyber Risk Assessment and Project Cybersecurity Plan. Include summary of lessons learned, if appropriate. Abide by grant award close-out T&Cs regarding disposition of assets built or purchased with grant award funding.
11	Grant Program Reporting and Review	Develop and document program lessons learned regarding cybersecurity. Review cybersecurity trends and patterns and identify updates to future NOFOs, standard grant award T&Cs, or other cybersecurity guidance.	None.

5 Model Language for Grant Programs

5.1 Model Language for Notice of Funding Opportunities (NOFOs)

The following language should be included in Federal agency NOFOs, or other notice of funding opportunities, to inform applicants of post-award cybersecurity requirements (this includes recipients making subawards):

> **"*Project Cyber Risk Assessment and Project Cybersecurity Plan*.** *Entities receiving funds through this program must ensure that cybersecurity is integrated into the design, development, operation, and maintenance of critical infrastructure information technology (IT) and operational technology (OT).*
>
> *Projects that contain and use programmable electronic devices essential to the reliable operation of critical infrastructure must complete certain requirements after receiving a grant award. These requirements include a Project Cyber Risk Assessment and a Project Cybersecurity Plan."*

5.2 Model Language for Award Terms and Conditions (T&Cs)

Federal agencies and recipients making subawards (PTEs) should include the following cybersecurity requirements in grant awards. Programs should tailor this language as needed when incorporating it into their award T&Cs. This includes a decision about whether to incorporate Project Cybersecurity Plan Attestation/Submission language - option 1 (self-attestation) or option 2 (Project Cybersecurity Plan submission and approval). The template below includes language for the:

- Project Cyber Risk Assessment
- Project Cybersecurity Plan
- Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update
- Project Cyber Risk Assessment and Project Cybersecurity Plan Closeout
- Project Cyber Risk Assessment and Project Cybersecurity Plan Attestation/Submission
- Actions to address non-compliance

"The Recipient shall conduct a Project Cyber Risk Assessment and Project Cybersecurity Plan during the project design phase and not later than [XX] months following issuance of award:

Project Cyber Risk Assessment. *Develop a Project Cyber Risk Assessment. Recipients may use the CISA Cybersecurity Performance Goal (CPG) Checklist Adapted for Grant Awards (Risk Assessment Tool) or use another assessment tool that meets or exceeds all CPG categories.*

Project Cybersecurity Plan. *Develop and maintain a Project Cybersecurity Plan. The plan shall include:*

(a) Section A. Administrative information.
(b) Section B. A high-level description of the plan for the overall management of the project's cybersecurity program, including a high-level description of how resources, roles, and responsibilities will be managed.
(c) Section C. Inventory of project IT/OT technology assets.
(d) Section D. A list of planned cybersecurity risk mitigation activities, including:
(i) A prioritized list of project cybersecurity gaps, based on the current Project Cyber Risk Assessment.
(ii) A target implementation date for each mitigation activity.

Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update. *The recipient is required to review and update, as appropriate, the Project Cyber Risk Assessment and Project Cybersecurity Plan annually. The updated assessment and plan must include all information in the initial/previous Plan, and as a minimum, updates to:*

Section C: Inventory of project IT/OT technology assets.
Section D: Planned cybersecurity actions with modifications, if any, including:
(i) Prioritized list of project cybersecurity gaps, based on the current Project Cyber Risk Assessment.
(ii) Planned cybersecurity mitigation activities with modifications, if any; and
(iii) The updated implementation date for each mitigation.

The Annual Update must contain sufficient information to demonstrate the recipient has taken appropriate actions to mitigate cybersecurity risks.

Project Cyber Risk Assessment and Project Cybersecurity Plan Closeout. *Critical infrastructure projects whose ownership will be transferred at the conclusion of the project must submit a Project Cybersecurity Plan Closeout to the entity receiving the transferred asset or operations. This includes all requirements of the Project Cyber Risk Assessment and Project Cybersecurity Plan Annual Update, and provides disposition instructions and system documentation (e.g., cybersecurity plan, any system manuals or guides, and system specifications) for transfer of critical infrastructure cyber asset(s) to entity receiving the transferred asset or operations.*

All Project Cyber Risk Assessment and Project Cybersecurity Plan and supporting information must be protected from unauthorized disclosure in accordance with applicable law and agency regulation. For technical data marked as proprietary by an entity, the agency must follow applicable law and agency regulation for the protection of such information, to include requests for information under the Freedom of Information Act (FOIA). Department and agency grant program managers will provide instructions to entities on the process for secure transmission of such assessments and plans, and ensure all information is maintained and stored in a protected system.

Some Project Cyber Risk Assessment and Project Cybersecurity Plan may be eligible for protection under the CISA Protected Critical Infrastructure Information (PCII) Program.[24] Federal awarding agencies may contact the CISA PCII Program Office for further information on how these protections might be extended to grantees.[25]

Project Cyber Risk Assessment and Project Cybersecurity Plan Attestation. *The recipient shall:*

(1) Self-attest that it has complied with the requirements for the development and maintenance of a Project Cyber Risk Assessment and Project Cybersecurity Plan. Additionally, recipients shall self-attest that they have developed and maintain an annual update of the Project Cyber Risk Assessment and Project Cybersecurity Plan. The annual update must contain sufficient information to demonstrate the recipient has taken corrective actions to resolve any previously identified cybersecurity compliance issues and concerns. Recipients shall provide (Federal agency/PTE) access to review the Project Cyber Risk Assessment and Project Cybersecurity Plan upon request.

or

(2) Submit the Project Cyber Risk Assessment and Project Cybersecurity Plan and annual updates within the timeframes specified. The annual updates must contain sufficient information to demonstrate the recipient has taken corrective actions to resolve any previously identified cybersecurity compliance issues and concerns.

If a recipient fails to comply with attestation or submission requirements, the grant agency may take one or more enforcement actions, which include disallowing costs, withholding further awards, or wholly or partly suspend the grant pending corrective action."

6 Grant Recipient Resources

6.1 Cyber Risk Assessment and Cybersecurity Performance Goals

Under the model language above, recipients may choose to use the *CISA Cybersecurity Performance Goal (CPG) Checklist Adapted for Grant Recipients (Cyber Risk Assessment Tool)* (see Appendix C), as a tool for conducting a Project Cyber Risk Assessment and developing and maintaining a Project Cybersecurity Plan.

Agencies should refer covered applicants and recipients to the cybersecurity resources and services, best practices, tools and training, and policy template resources in the Appendices to enable recipient development, implementation, and maintenance of Cybersecurity Plan. The resources in Appendix E are organized by CPG to guide grant recipients to the resource(s) that are most useful for addressing their CPG gaps and needs.

---

[24] Please visit CISA's website for more information about the PCII Program at https://www.cisa.gov/resources-tools/programs/protected-critical-infrastructure-information-pcii-program.

[25] Grant program managers are encouraged to work within their Agencies and with their respective Chief Information Officer (CIO) or Chief Information Security Officer (CISO) to develop and provide guidance to grantees regarding the collection and storage of sensitive data.

Agencies and grant PMs should encourage covered award applicants and recipient organizations that have implemented mature cybersecurity best practices and controls (and who may have already implemented CPGs at an organizational level) to continue strengthening their cross-sector and sector-specific cybersecurity best practices and controls by implementing the *NIST Cybersecurity Framework.*[26]

Under the model language above, recipients may use the *CISA CPG Checklist Adapted for Grant Recipients (Cyber Risk Assessment Tool)* when performing project and organization cyber risk assessments. Project-level assessments include cybersecurity best practices and controls of any IT/OT assets proposed to be designed, developed, operated, or maintained with grant award project funding. The project assessment should include the cyber assets controlled as part of the execution of the project. An assessment of the cybersecurity best practices of the grant recipient organization, parent organization, and partner organizations is strongly recommended, but not required.

The initial Project Cyber Risk Assessment and associated Project Cybersecurity Plan should be attested to or submitted within the timeframe established in grant award terms and conditions. Subsequent Project Cyber Risk Assessments performed as part of updating the Project Cybersecurity Plan should be completed annually.

The column in the Cyber Risk Assessment Tool titled "Risk Addressed" references specific risks and tactics, techniques, and procedures outlined in the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, a widely used reference for addressing cyber risks and threats.[27]

Note: A Microsoft Excel spreadsheet with the below information is available as a companion document for ease of conducting the Project Cyber Risk Assessment and in developing and maintaining the Project Cybersecurity Plan.

7 Conclusion

Investments to the cybersecurity of our critical infrastructure is key to preventing disruption and minimizing potential negative impacts. Grant programs funded by the IIJA and other investments present the opportunity—and necessity—to build cybersecurity into the critical infrastructure projects they fund. Critical infrastructure must therefore be developed and updated by incorporating the concepts of cyber-informed engineering and secure by design. Incorporating baseline security practices is vital to protect national and economic security and ensure a safe and prosperous future for all Americans.

[26] https://www.nist.gov/cyberframework

[27] MITRE ATT&CK Framework, https://attack.mitre.org/.

Appendix A List of Acronyms

Acronym	Definition
CI	Critical Infrastructure
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cybersecurity Performance Goal
ICS	Industrial Control System
IIJA	Infrastructure Investment and Jobs Act
IRA	Inflation Reduction Act
IT	Information Technology
NOFO	Notice of Funding Opportunity
OMB	Office of Management and Budget
ONCD	Office of the National Cyber Director
OT	Operational Technology
PM	Program Manager
PTE	Pass-Through Entity
T&C	Terms and Conditions

Appendix B Glossary of Terms

Term	Definition
Critical Cyber Asset	Any programmable electronic devices, including the hardware, software, and data in those devices, essential to the reliable operation of facilities, systems, and equipment which, if destroyed, degraded, or otherwise rendered unavailable, would affect the reliability or operability of critical infrastructure. Critical cyber assets may include elements, components, and full systems of IT, OT, ICS, SCADA, and other systems. (Derived from NERC, NIST, and CISA)
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. 42 USC 5195c(e)
Cyber Risk	Risk of financial loss, operational disruption, or damage, from the failure of the digital technologies employed for informational and/or operational functions introduced to a manufacturing system via electronic means from the unauthorized access, use, disclosure, disruption, modification, or destruction of the manufacturing system. (https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.8183A-3.pdf)
Cybersecurity	Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. (NIST SP 1800-10)
Industrial Control System	An information system used to control industrial processes such as manufacturing, product handling, production, and distribution. Industrial control systems include supervisory control and data acquisition systems used to control geographically dispersed assets, as well as distributed control systems and smaller control systems using programmable logic controllers to control localized processes. (NIST SP 800-30 Rev. 1)
Industrial Internet of Things (IIoT)	The sensors, instruments, machines, and other devices that are networked together and use Internet connectivity to enhance industrial and manufacturing business processes and applications. (NIST SP 800-172)
Information System	A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This includes industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers. (6 U.S.C. § 650(14))
National Critical Functions	Risk Management National Critical Functions (NCFs) are functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof. https://www.cisa.gov/.
Operational Technology	Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms. (NIST SP 800-37 Rev. 2)
Security Control	The means of managing risk, including policies, procedures, guidelines, best practices, or organizational structures, which can be of an administrative, technical, management, or legal nature. (NIST SP 800-160 Vol. 2 Rev. 1)

Appendix C CISA CPG Checklist Adapted for Grant Recipients (Cyber Risk Assessment Tool)

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
Identify	1.A	Asset Inventory	Hardware Additions (T1200) Exploit Public-Facing Application (T0819, ICS T0819) Internet Accessible Device (ICS T0883)	Maintain a regularly updated project inventory of all project assets with an IP address (including IPv6), including OT. Ensure project assets are included in the organizational inventory and updated on a recurring basis, no less than monthly, for both IT and OT.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly, for both IT and OT.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Identify	1.B	Organizational Cybersecurity Leadership	Lack of sufficient cybersecurity accountability, investment, or effectiveness.	A named project role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the system level, identifying and requesting project cybersecurity budget resources, or leading the project cybersecurity strategy.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Identify	1.C	OT Cybersecurity Leadership	A single leader is responsible and accountable for OT-specific cybersecurity within	A named project role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some	Date: □ Implemented □ In Progress □ Scoped □ Not Started	A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations this may	Date: □ Implemented □ In Progress □ Scoped □ Not Started

[28] MITRE ATT&CK Framework, https://attack.mitre.org/

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
			an organization with OT assets.	projects this may be the same position as identified in 1. B.		be the same position as identified in 1. B.	
Identify	1.D	Improving IT and OT Cybersecurity Relationships	Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.	Sponsor at least one social gathering per year that is focused on strengthening working relationships between project IT and OT security personnel; this is not a working event (such as providing meals during an incident response).	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations sponsor at least one meeting or event per year that is focused on strengthening working relationships between IT and OT security personnel.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Identify	1.E	Mitigating Known Vulnerabilities	Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) Supply Chain Compromise (T1195, ICS T0862) External Remote Services (T1133, ICS T0822)	All known exploited vulnerabilities (listed in CISA's KEV catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For OT assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls should either make the project asset inaccessible from the public internet or reduce the ability of adversaries to exploit the	Date: □ Implemented □ In Progress □ Scoped □ Not Started	All known exploited vulnerabilities (listed in CISA's KEV catalog - https://www.cisa.gov/known-exploited-vulnerabilities-catalog) in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first. OT: For OT assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls should either make the asset inaccessible from the public internet or reduce the ability of adversaries to exploit the vulnerabilities in these assets.	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				vulnerabilities in these project assets.			
Identify	1.F	Third-Party Validation of Cybersecurity Control Effectiveness	Reduce risk of gaps in cyber defenses or a false sense of security in existing protections.	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of a project's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical (including OT/ICS) systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests. Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical (including OT/ICS) systems. High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Identify	1.G	Supply Chain Incident Reporting	Supply Chain Compromise (T1195, ICS T0862)	Procurement documents and contracts, such as Service Level Agreements (SLAs), stipulate that vendor and/or service providers notify the procuring customer of	Date: □ Implemented □ In Progress □ Scoped	Procurement documents and contracts, such as Service Level Agreements (SLAs), stipulate that vendor and/or service providers notify the procuring customer of	Date: □ Implemented □ In Progress □ Scoped

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				security incidents within a risk-informed timeframe as determined by the customer.	□ Not Started	security incidents within a risk-informed timeframe as determined by the organization.	□ Not Started
Identify	1.H	Supply Chain Vulnerability Disclosure	Supply Chain Compromise (T1195, ICS T0862)	Procurement documents and contracts, such as Service Level Agreements (SLAs), stipulate that vendor and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed timeframe as determined by the customer.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Procurement documents and contracts, such as Service Level Agreements (SLAs), stipulate that vendor and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed timeframe as determined by the organization.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Identify	1.I	Vendor/Supplier Cybersecurity Requirements	Supply Chain Compromise (T1195, ICS T0862)	Procurement documents include cybersecurity requirements and questions, which are evaluated during vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.A	Changing Default Passwords	Valid Accounts - Default Accounts (T1078.001) Valid Accounts (ICS T0859)	Project manager attests that policy and/or process is followed that addresses changing default manufacturer passwords for any/all hardware, software, and firmware before being put on any internal or external network. This includes IT assets for OT, such as OT administration web pages. In instances where changing default passwords is not feasible	Date: □ Implemented □ In Progress □ Scoped □ Not Started	An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before being put on any internal or external network. This includes IT assets for OT, such as OT administration web pages. In instances where changing default passwords is not feasible	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				(e.g., a control system with a hard-coded password), project manager attests to implementing and documenting appropriate compensating security controls, and monitoring logs for network traffic and login attempts on those devices. OT: While changing default passwords on a project's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversaries' TTPs change.		(e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices. OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversaries' TTPs change.	
Protect	2.B	Minimum Password Strength	Brute Force - Password Guessing (T1110.001) Brute Force - Password Cracking (T1110.002) Brute Force - Password Spraying (T1110.003) Brute Force - Credential Stuffing (T1110.004)	Require a minimum password length of 15* or more characters for all password protected project IT assets and project OT assets where technically possible. ** Consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Project assets that	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password protected IT assets and all OT assets where technically possible. ** Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. This goal is particularly important when project implementation of MFA and capabilities to protect against brute force attacks are lacking (such as Web Application Firewalls and third-party Content Delivery Networks) or when password-less authentication methods are not adopted. * Modern attacker tools can crack 8-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations and makes it easier for humans to create and remember passwords. ** Project OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as		login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength length are prioritized for upgrade or replacement. This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute force attacks (such as Web Application Firewalls and third-party Content Delivery Networks) or are unable to adopt password-less authentication methods. * Modern attacker tools can crack 8-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations and makes it easier for humans to create and remember passwords. ** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on	

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				those on offshore rigs or on top of wind turbines.		offshore rigs or on top of wind turbines.	
Protect	2.C	Unique Credentials	Valid Accounts (T1078, ICS T0859) Brute Force - Password Guessing (T1110.001)	Unique and separate credentials are provisioned for similar services and asset access on project IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have unique passwords from all member user accounts.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have unique passwords from all member user accounts.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.D	Revoking Credentials for Departing Employees	Valid Accounts (T1078, ICS T0859)	For all staff departing the project, assess needs for access in the next role. (1) Revoke and securely return all unneeded physical badges, key cards, tokens, etc., and (2) disable all unneeded user accounts and access to project resources.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	A defined and enforced administrative process applied to all departing employees by the day of their departure that: (1) revokes and securely return all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.E	Separating User and Privileged Accounts	Valid Accounts (T1078, ICS T0859)	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are revaluated on a recurring basis to validate continued need for a given set of permissions.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are revaluated on a recurring basis to validate continued need for a given set of permissions.	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
Protect	2.F	Network Segmentation	Network Service Discovery (T1046) Trusted Relationship (T1199) Network Connection Enumeration (ICS T0840) Network Sniffing (T1040, ICS T0842)	All connections to the project OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the project IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone (DMZ), which is closely monitored, captures network logs, and only allows connections from approved assets.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.G	Detection of Unsuccessful (Automated) Login Attempts	Brute Force - Password Guessing (T1110.001) Brute Force - Password Cracking (T1110.002) Brute Force - Password Spraying (T1110.003) Brute Force - Credential Stuffing (T1110.004)	All unsuccessful logins are logged and sent to a relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts over two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, there is a system-enforced policy that prevents future logins for the suspicious account. For example, this could be for some minimum time, or	Date: □ Implemented □ In Progress □ Scoped □ Not Started	All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts over two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis. For IT assets, there is a system-enforced policy that prevents future logins for the suspicious account. For example, this could	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins over a 10-minute period.		be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10 minutes after 10 incorrect logins over a 10-minute period.	
Protect	2.H	Phishing-Resistant Multifactor Authentication (MFA)	Brute Force (T1110) Remote Services - Remote Desktop Protocol (T1021.001) Remote Services - SSH (T1021.004) Valid Accounts (T1078, ICS T0859) External Remote Services (ICS T0822)	Hardware-based MFA is enabled when available; if not, then soft tokens (such as via mobile app) should be used. MFA via SMS should only be used when no other options are possible. IT: IT accounts leverage multi-factor authentication to access project resources. OT: Within project OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible Human Machine Interfaces (HMIs).	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Hardware-based MFA is enabled when available; if not, then soft tokens (such as via mobile app) should be used. MFA via SMS should only be used when no other options are possible. IT: IT accounts leverage multi-factor authentication to access organizational resources. OT: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible Human Machine Interfaces (HMIs).	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.I	Basic Cybersecurity Training	User Training (M1017, ICS M0917)	At a minimum, conduct annual trainings for all project staff and contractors that covers basic security concepts, such as phishing, business email	Date: □ Implemented □ In Progress □ Scoped	At least annual trainings for all organizational staff contractors that covers basic security concepts, such as phishing, business email compromise,	Date: □ Implemented □ In Progress □ Scoped

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				compromise, basic operational security (OPSEC), password security, etc., as well as fostering a culture of security and cybersecurity awareness. New project staff receive initial cybersecurity training within 10 days of onboarding, and recurring training on at least an annual basis.	□ Not Started	basic operational security (OPSEC), password security, etc., as well as fostering an internal culture of security and cybersecurity awareness. New employees receive initial cybersecurity training within 10 days of onboarding, and recurring training on at least an annual basis.	□ Not Started
Protect	2.J	OT Cybersecurity Training	User Training (M1017, ICS M0917)	In addition to basic cybersecurity training, project personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.K	Strong and Agile Encryption	Adversary-in-the-Middle (T1557) Automated Collection (T1119) Network Sniffing (T1040, ICS T0842) Wireless Compromise (ICS T0860) Wireless Sniffing (ICS T0887)	Properly configured and up-to-date secure socket layer (SSL)/ transport layer security (TLS) is utilized to protect data in transit where technically feasible. Projects should also plan for identifying any use of outdated or weak encryption and updating to sufficiently strong algorithms, and consideration for managing the implications of post-quantum cryptography. OT: To minimize the impact to latency and availability; encryption is used where feasible, usually for OT	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Properly configured and up-to-date secure socket layer (SSL)/ transport layer security (TLS) is utilized to protect data in transit where technically feasible. Organizations should also plan on identifying any use of outdated or weak encryption and updating to sufficiently strong algorithms, and consideration for managing the implications of post-quantum cryptography. OT: To minimize the impact to latency and availability; encryption is used where feasible, usually for OT	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				communications connecting with remote/external assets.		communications connecting with remote/external assets.	
Protect	2.L	Secure Sensitive Data	Unsecured Credentials (T1552) Steal or Forge Kerberos Tickets (T1558) OS Credential Dumping (T1003) Data from Information Repositories (ICS T0811) Theft of Operational Information (T0882)	Sensitive data, including credentials, are not stored in plaintext anywhere, and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Sensitive data, including credentials, are not stored in plaintext anywhere in the organization, and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.M	Email Security	Phishing (T1566) Business Email Compromise	On all project email infrastructure: (1) STARTTLS is enabled, (2) SPF and DKIM are enabled, and (3) DMARC is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies at: https://www.cisa.gov/binding-operational-directive-18-01	Date: □ Implemented □ In Progress □ Scoped □ Not Started	On all corporate email infrastructure: (1) STARTTLS is enabled, (2) SPF and DKIM are enabled, and (3) DMARC is enabled and set to "reject." For further examples and information, see CISA's past guidance for federal agencies at: https://www.cisa.gov/binding-operational-directive-18-01	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.N	Disable Macros by Default	Phishing - Spear phishing Attachment (T1566.001)	A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, authorized users	Date: □ Implemented □ In Progress □ Scoped □ Not Started	A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
			User Execution - Malicious File (T1204.002)	request that macros are enabled on specific assets.		that macros are enabled on specific assets.	
Protect	2.O	Document Device Configurations	Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.	Maintain accurate documentation describing the baseline and current configuration details of project critical IT and OT assets to facilitate more effective vulnerability management and response & recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response & recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.P	Document Network Topology	Incomplete or inaccurate understanding of network topology inhibits effective incident response and recovery.	Maintain accurate documentation describing updated network topology and relevant information across project IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.Q	Hardware and Software Approval Process	Supply Chain Compromise (T1195, ICS T0862) Hardware Additions (T1200) Browser Extensions (T1176) Transient Cyber Asset (ICS T0864)	Require approval before new hardware, firmware, or software/software version is installed or deployed. Maintain a risk-informed allow list of approved hardware, firmware, and software to include specification of approved versions when technically feasible. For OT assets specifically, these actions should	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allow list of approved hardware, firmware, and software to include specification of approved versions when	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				also be aligned with defined change control and testing activities.		technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.	
Protect	2.R	System Backups	Data Destruction (T1485, ICS T0809) Data Encrypted for Impact (T1486) Disk Wipe (T1561) Inhibit System Recovery (T1490) Denial of Control (ICS T0813) Denial/Loss of View (ICS T0815, T0829) Loss of Availability (T0826) Loss/Manipulation of Control (T0828, T0831)	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for project OT assets includes at a minimum: configurations, roles, PLC logic, engineering drawings, and tools.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, PLC logic, engineering drawings, and tools.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.S	Incident Response (IR) Plans	Inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents.	Identify, maintain, update, and regularly drill project IT and OT cybersecurity incident response plans for both common and project-specific (e.g., by sector, locality, etc.) threat scenarios and TTPs. When conducted, tests or drills are as realistic in nature as feasible. IR plans are drilled at least annually and are updated within a risk-informed time	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations have, maintain, updated, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally specific (e.g., by sector, locality, etc.) threat scenarios and TTPs. When conducted, tests or drills are as realistic in nature as feasible. IR plans are drilled at least annually and are updated within a risk-	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				frame following the lessons learned portion of any exercise or drill.		informed time frame following the lessons learned portion of any exercise or drill.	
Protect	2.T	Log Collection	Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents Impair Defenses (T1562)	Access and security focused (e.g., IDS/IDPS, firewall, DLP, VPN) logs are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Access and security focused (e.g., IDS/IDPS, firewall, DLP, VPN) logs are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging. OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.U	Secure Log Storage	Indicator Removal on Host – Clear Windows Event Logs (T1070.001) Indicator Removal on Host – Clear Linux or Mac System Logs (T1070.002) Indicator Removal on Host – File Deletion (T1070.004) Indicator Removal on Host (ICS T0872)	Logs are stored in a central system, such as a Security Information and Event Management (SIEM) tool or central database and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Logs are stored in a central system, such as a Security Information and Event Management (SIEM) tool or central database and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
Protect	2.V	Prohibit Connection of Unauthorized Devices	Hardware Additions (T1200) Replication Through Removable Media (T1091, ICS T0847)	Ensure that unauthorized media and hardware are not connected to project IT and OT assets, such as by limiting use of USB devices and removable media or disabling Autorun. OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as by limiting use of USB devices and removable media or disabling Autorun. OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices, or establish procedures for granting access through approved exceptions.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Protect	2.W	No Exploitable Services on the Internet	Active Scanning – Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) External Remote Services (T1133, ICS T0822) Remote Services – Remote Desktop Protocol (T1021.001)	Project assets on the public internet expose no exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing project assets.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Assets on the public internet expose no exploitable services, such as RDP. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing project assets.	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
Protect	2.X	Limit OT Connections to Public Internet	Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) External Remote Services (T1133, ICS T0822) Loss/Manipulation of Control (T0828, T0831)	No project OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted project assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or another intermediary, etc.).	Date: □ Implemented □ In Progress □ Scoped □ Not Started	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or another intermediary, etc.).	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Detect	3.A	Detecting Relevant Threats and TTPs	Without the knowledge of relevant threats and ability to detect them, organizations risk that threat actors may exist undetected in their networks for long periods.	Document a list of relevant threats and adversary TTPs relevant to the project (based on industry, sectors, etc.), and have the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations have documented a list of threats and adversary TTPs relevant to their organization (based on industry, sectors, etc.), and have the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Respond	4.A	Incident Reporting	Without timely incident reporting, CISA and other groups are less able to assist affected organizations and	Report all confirmed cybersecurity incidents to appropriate external entities (e.g., State/Federal regulators or SRMA's as required, as well as CISA).	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Organizations maintain codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., State/Federal	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
			lack critical insight into the broader threat landscape (such as whether a broader attack is occurring against a specific sector).	Known incidents are reported to CISA as well as other necessary parties within timeframes directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).		regulators or SRMA's as required, ISAC/ISAO, as well as CISA). Known incidents are reported to CISA as well as other necessary parties within timeframes directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).	
Respond	4.B	Vulnerability Disclosure/Reporting	Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) Supply Chain Compromise (T1195, ICS T0862)	Consistent with NIST SP 800-53 Revision 5, project maintains a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity.	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Category	ID	Security Practice	Risk Addressed (MITRE ATT&CK Framework [28])	Recommended Action for Recipient Project	Recipient Project Assessment	Recommended Action for Organization(s)	Recipient Organization Assessment
				Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules.		Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules.	
Respond	4.C	Deploy Security.txt Files	Active Scanning - Vulnerability Scanning (T1595.002) Exploit Public-Facing Application (T1190, ICS T0819) Exploitation of Remote Service (T1210, ICS T0866) Supply Chain Compromise (T1195, ICS T0862)	All project public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.	Date: □ Implemented □ In Progress □ Scoped □ Not Started
Recover	5.A	Incident Planning and Preparedness	Disruption to availability of an asset, service, or system.	Develop, maintain, and execute plans to recover and restore to service project- or mission-critical assets or systems that might be impacted by a cybersecurity incident.	Date: □ Implemented □ In Progress □ Scoped □ Not Started	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.	Date: □ Implemented □ In Progress □ Scoped □ Not Started

Appendix D Project Cyber Risk Assessment and Cybersecurity Plan Sample Templates[29]

Grant program managers and award recipients can use templates below to create their own Project Cyber Risk Assessment and Project Cybersecurity Plan. This tool allows for risk management practices to be identified and prioritized throughout the project's lifecycle. The risk assessment tool is based on CISA's Cybersecurity Performance Goals (CPGs), and is provided in detail in Appendix C and in a companion MS Excel Spreadsheet for ease of use.[30]

Template Version 1:

Project Cyber Risk Assessment

Section I: Identify

A. Asset Inventory
B. Organizational Cybersecurity Leadership
C. OT Cybersecurity Leadership
D. Improving IT and OT Cybersecurity Relationships
E. Mitigating Known Vulnerabilities
F. Third-Party Validation of Cybersecurity Control Effectiveness
G. Supply Chain Incident Reporting
H. Supply Chain Vulnerability Disclosure
I. Vendor/Supplier Cybersecurity Requirements

Section II: Protect

A. Changing Default Passwords
B. Minimum Password Strength
C. Unique Credentials
D. Revoking Credentials for Departing Employees
E. Separating User and Privileged Accounts
F. Network Segmentation
G. Detection of Unsuccessful (Automated) Login Attempts
H. Phishing-Resistant Multifactor Authentication (MFA)
I. Basic Cybersecurity Training
J. OT Cybersecurity Training
K. Strong and Agile Encryption
L. Secure Sensitive Data
M. Email Security
N. Disable Macros by Default
O. Document Device Configurations
P. Document Network Topology
Q. Hardware and Software Approval Process
R. System Backups

[29] Note: A companion Microsoft Excel fillable worksheet of this template is available for use in developing the Project Cyber Risk Assessment and Project Cybersecurity Plan.

[30] CISA CPG: Cross-Sector Cybersecurity Performance Goals, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals.

S. Incident Response (IR) Plans
T. Log Collection
U. Secure Log Storage
V. Prohibit Connection of Unauthorized Devices
W. No Exploitable Services on the Internet
X. Limit OT Connections to Public Internet

Section III: Detect

A. Document a list of threats and cyber actor tactics, techniques, and procedures (TTPs)

Section IV: Respond

A. Incident Reporting
B. Vulnerability Disclosure/Reporting
C. Deploy Security.TXT Files

Section V: Recover

A. Incident Planning and Preparedness

Project Cybersecurity Plan

A. Grant Award Information
1. *Federal Award ID Number*
2. *Recipient Name*
3. *Fiscal Funding Year*
4. *Project Title*
5. *Project Type*
6. *Plan Completed By (Point of Contact Name)*
7. *Point of Contact*
    - *Title*
    - *Point of Contact Email*
    - *Point of Contact Phone Number*

B. Description of Overall Management of Project Cybersecurity Program

C. Inventory of project IT/OT Technology Assets

D. Planned Cybersecurity Risk Mitigation Actions
1. *Prioritized list of project cybersecurity gaps.*
2. *Project cybersecurity risk mitigations with a target implementation date for each mitigation.*

Sample Project Cybersecurity Plan Template Version 2 (Note: A companion MS Excel Spreadsheet available for use)		
A. Grant Award Information		
Federal Award ID Number (FAIN)	Recipient Name	Fiscal Funding Year
Project Title	Project Type	Plan Completed By (Point of Contact Name)
Point of Contact Title	Point of Contact Email	Point of Contact Phone Number
☐ Attestation: By checking this box, I attest that I have reviewed this plan and that, to the best of my knowledge, the plan is complete, accurate and meets the terms and conditions of the award.		
B. Description of Overall Management of Project Cybersecurity Program		
C: Inventory of IT/OT Assets		
D. Cybersecurity Risk Mitigation Actions[31]		

Planned Cybersecurity Risk Mitigation Actions (Dates in YYYY/MM/DD)											Current Mitigation Action Status			
a.	b.	c.	d.	e.	f.	g.	h.	i.	j.	k.	L.	m.	n.	o.
ID[32]	Security Practice Gap[33]	Level[34]	Priority[35]	Initial Status[36]	Planned Mitigation Action(s)	Personnel Responsible	Involved Organizations/ Departments	Planned Start Date	Planned Completion Date	Plan Notes[37]	Current Status[38]	Start Date	Completion Date	Progress Notes[39]

[31] Columns "l" through "o" should be left blank for the initial cybersecurity plan and populated for updated Project Cybersecurity Plans.

[32] The "ID" should match the ID of the security practice listed in the *CISA CPG Checklist Adapted for Grant Awards* (*Cyber Risk Assessment Tool*).

[34] Valid values for the "Level" column include the following: Grant Award Project, Grant Recipient Organization, Parent Organization, or Partner Organization.

[34] Valid values for the "Level" column include the following: Grant Award Project, Grant Recipient Organization, Parent Organization, or Partner Organization.

[35] Valid values for the "Priority" include the following: High, Medium, or Low.

[36] Valid values for the "Initial Status" column include the following: Scoped, Not Started, In Progress, or Implemented.

[37] "Plan Notes" should include a description of and rationale for any additions, modifications, or deletions to planned mitigation actions.

[38] Valid values for the "Current Status" column include the following: Scoped, Not Started, In Progress, or Implemented.

[39] "Progress Notes" should include a description of and rationale for any planned mitigation actions that were not started or completed by the planned dates.

Appendix E Cybersecurity Resources for Grant Recipient Project Development and Execution

The resources in this appendix support grant applicants and recipients in their development and maintenance of Cybersecurity Plans.

Cyber Hygiene Vulnerability Scanning. All applicants and recipients should sign up for CISA's no-cost Cyber Hygiene Vulnerability Scanning.[40] Vulnerability scanning helps secure internet-facing systems from weak configurations and known vulnerabilities and encourages the adoption of best practices. Once enrolled, CISA will perform vulnerability scans and deliver appropriate reports. Additional information can be found at: https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning. Interested parties may request this service by emailing vulnerability@cisa.dhs.gov.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Identify (ID)	1.A	Asset Inventory	CIS Vulnerability Assessments https://www.cisecurity.org/services/vulnerability-assessments [FEE-BASED]	CISA Stuff Off Search https://www.cisa.gov/resources-tools/resources/stuff-search National Cybersecurity Alliance: https://staysafeonline.org/cybersecurity-for-business/identify-your-crown-jewels/	CIS Hardware and Software Asset Tracking Spreadsheet https://www.cisecurity.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet AT&T AlienVault OSSIM https://cybersecurity.att.com/products/ossim	CIS Planning Policy https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17 Enterprise Asset Management Policy Template https://www.cisecurity.org/insights/white-papers/enterprise-asset-management-policy-template

[40] CISA: Vulnerability Scanning, https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning.

[41] The policy templates included in this resource guide were obtained from the SANS Security Policy Project (https://www.sans.org/information-security-policy/) and the MS-ISAC Cybersecurity Resources Guide (https://www.cisecurity.org/wp-content/uploads/2020/07/MS-ISAC-Cybersecurity-Resources-Guide-2020-0720.pdf). The templates provide a baseline that can be customized based on the specific cybersecurity requirements of a project or organization. For more extensive policy documents, the sections relevant to the CPG have been noted.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Identify (ID)	1.B	Organizational Cybersecurity Leadership	None identified.	CISA Security Tip: Questions Every CEO should Ask about Cyber Risks https://www.cisa.gov/news-events/news/questions-every-ceo-should-ask-about-cyber-risks#:~:text=CEOs%20should%20ask%20the%20following%20questions%20about%20potential,resiliency%20to%20minimize%20our%20cybersecurity%20risks%3F%20More%20items DHS Cybersecurity Questions for CEOs https://www.cisa.gov/news-events/news/questions-every-ceo-should-ask-about-cyber-risks#:~:text=The%20following%20questions%20will%20help%20CEOs%20guide%20discussions,training%20is%20available%20for%20our%20workforce%3F%20More%20items	Cynet's Security Budget Plan and Track Template https://go.cynet.com/the-ultimate-security-budget-template SANS Cybersecurity Leadership Curriculum https://www.sans.org/blog/sans-cybersecurity-leadership-curriculum/	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				Workforce Framework for Cybersecurity https://niccs.cisa.gov/workforce-development/nice-framework Workforce Framework for Cybersecurity: Cybersecurity Management https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cybersecurity-management Workforce Framework for Cybersecurity: Executive Cyber Leadership https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/executive-cyber-leadership Workforce Framework for Cybersecurity: Strategic Planning and Policy https://niccs.cisa.gov/workforce-development/nice-		

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				framework/specialty-areas/strategic-planning-and-policy		
Identify (ID)	1.C	OT Cybersecurity Leadership	None identified.	CISA Security Tip: Questions Every CEO should Ask about Cyber Risks https://www.cisa.gov/news-events/news/questions-every-ceo-should-ask-about-cyber-risks#:~:text=The%20following%20questions%20will%20help%20CEOs%20guide%20discussions,training%20is%20available%20for%20our%20workforce%3F%20More%20items CISA's ICS Cybersecurity for the C-Level Fact Sheet https://www.cisa.gov/sites/default/files/FactSheets/NCCIC%20ICS_FactSheet_ICS_Cybersecurity_C-Level_S508C.pdf CISA Workforce Framework for Cybersecurity https://niccs.cisa.gov/	SANS Cybersecurity Leadership Curriculum https://www.sans.org/blog/sans-cybersecurity-leadership-curriculum/	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				workforce-development/nice-framework CISA Workforce Framework for Cybersecurity: Cybersecurity Management https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/cybersecurity-management Workforce Framework for Cybersecurity: Executive Cyber Leadership https://niccs.cisa.gov/workforce-development/nice-framework/specialty-areas/executive-cyber-leadership CISA Workforce Framework for Cybersecurity: Strategic Planning and Policy https://niccs.cisa.gov/workforce-development/nice-framework/specialty-		

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				areas/strategic-planning-and-policy		
Identify (ID)	1.D	Improving IT and OT Cybersecurity Relationships	None identified.	None identified.	None identified.	None identified.
Identify (ID)	1.E	Mitigating Known Vulnerabilities	CIS Vulnerability Assessments https://www.cisecurity.org/services/vulnerability-assessments [FEE-BASED] FortifyData https://fortifydata.com/cisa-free-tools-threat-exposure-ratings/	CISA Alerts https://www.cisa.gov/news-events/cybersecurity-advisories Known Exploited Vulnerabilities (KEV) Catalog https://www.cisa.gov/known-exploited-vulnerabilities-catalog NIST National Vulnerability Database https://nvd.nist.gov/ VulnRX https://vulcan.io/voyager-18/	CISA Cyber Hygiene Services https://www.cisa.gov/cyber-hygiene-services	CIS Vulnerability Management Policy Template https://www.cisecurity.org/controls/v8
Identify (ID)	1.F	Third Party Validation of Cybersecurity Control Effectiveness	CIS Penetration Testing https://www.cisecurity.org/controls/penetration-testing [FEE-BASED] National Council of ISACs https://www.nationali	CISA Tabletop Exercise Packages https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages#:~:text=CISA%20Tabletop%20Exercise%20Packages%201	CISA Cyber Security Evaluation Tool https://www.cisa.gov/downloading-and-installing-cset	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
			sacs.org/about-isacs [FEE-BASED]	%20Cybersecurity%20Scenarios%20These,Cyber-Physical%20Convergence%20Scenarios%20...%204%20CTEP%20Documents%20 CIS Tabletop Exercises https://www.cisecurity.org/ms-isac/tabletop-exercises-ttx		
Identify (ID)	1.G	Supply Chain Incident Reporting	None identified.	CISA Cyber Incident Detection and Notification Planning Guide https://www.cisa.gov/resources-tools/resources/cyber-incident-detection-and-notification-planning-guide Sharing Cyber Event Information: Observe, Act, Report https://www.cisa.gov/resources-tools/resources/sharing-cyber-event-information-observe-act-report	None identified.	Law Insider Incident Reporting Sample Clause https://www.lawinsider.com/clause/incident-reporting SANS Cybersecurity Incident Response Contact Details https://www.sans.org/digital-forensics-incident-response/ (Fee Based) CDN Cybersecurity Incident Response Incident Summary Template https://cdn.fedweb.org/fed-34/2/Cyber-Security-Incident-

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
						Response-Template.pdf
Identify (ID)	1.H	Supply Chain Vulnerability Disclosure	None identified.	PNNL Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28661.pdf OWASP Vulnerability Disclosure Cheat Sheet https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html	None identified.	Department of Energy (DOE) Cybersecurity Procurement Language (Section 3.3) https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014
Identify (ID)	1.I	Vendor/ Supplier Cybersecurity Requirements	None identified.	Guide on Cybersecurity Procurement Language in Task Order Requests for Proposals for Federal Facilities https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-28661.pdf OWASP Vulnerability Disclosure Cheat Sheet	Federal Energy Management Plan Cybersecurity for Procurement Process Decision Tree https://www.energy.gov/femp/cybersecurity-considerations-procurement	Department of Energy (DOE) Cybersecurity Procurement Language (Section 3.3) https://www.energy.gov/ceser/articles/cybersecurity-procurement-language-energy-delivery-april-2014 CIS White Papers

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				https://cheatsheetseries.owasp.org/cheatsheets/Vulnerability_Disclosure_Cheat_Sheet.html FTC's Small Business Vendor Security https://www.ftc.gov/business-guidance/small-businesses/cybersecurity/vendor-security List of Covered Equipment and Services https://www.fcc.gov/supplychain/coveredlist The Open Group - Open Trusted Technology Provider Standard https://www.opengroup.org/certifications/o-ttps MS-ISAC Supply Chain Cybersecurity Resources Guide https://www.cisecurity.org/wp-content/uploads/2021/02/Supply-Chain-Cybersecurity-Resources-Guide.pdf		https://www.cisecurity.org/insights/white-papers

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.A	Changing Default Passwords	None identified.	CISA Bad Practices https://www.cisa.gov/news-events/news/bad-practices-0 CIS Password Policy Guide (See Section 5.1.6 & 5.1.7) https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide	None identified.	SANS Password Protection Policy https://www.sans.org/information-security-policy/ https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/bltf5d5757503e36442/636f1a316bafb12e165da155/Password_Protection_Policy.pdf
Protect (PR)	2.B	Minimum Password Strength	None identified.	CIS Password Policy Guide (See Sections 3, 5.1.1, 5.2.1, 5.2.1, & 5.2.3) https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide CISA Bad Practices https://www.cisa.gov/news-events/news/bad-practices-0 CISA Security Tip: Choosing and Protecting Passwords https://www.cisa.gov/news-events/news/choosing	CISA Bad Practices Discussion Page (GitHub) https://github.com/cisagov/bad-practices/discussions Cyber Readiness Institute: The Cyber Readiness Program https://cyberreadinessinstitute.org/ Security.Org - How Secure is My Password? https://www.security.org/how-secure-is-my-password/ MS-ISAC - Establishing Essential Cyber Hygiene	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				-and-protecting-passwords Password Guidance from NIST https://www.nist.gov/video/password-guidance-nist-0	https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene	
Protect (PR)	2.C	Unique Credentials	None identified.	CISA - Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies (pg. 25, Section 2.5.4) https://www.cisa.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf	Cyber Readiness Institute: The Cyber Readiness Program https://cyberreadinessinstitute.org/	SANS Password Protection Policy (See Section 4.1) https://www.sans.org/blog/everything-you-need-to-know-about-passwords-for-your-organization/
Protect (PR)	2.D	Revoking Credentials for Departing Employees	None identified.	WaterISAC - 15 Cybersecurity Fundamentals for Water and Wastewater Utilities (pg. 17) https://www.waterisac.org/fundamentals	None identified.	CIS – MS-ISAC Establishing Essential Cyber Hygiene https://www.cisecurity.org/insights/white-papers/establishing-essential-cyber-hygiene CIS Information Security Policy Templates https://www.cisecurity.org/controls/v8

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.E	Separating User and Privileged Accounts	None identified.	Center for Internet Security Access Control Policy https://www.cisecurity.org/controls/access-control-management NIST SP 800-82 Guide to Industrial Control Systems (Section 6.2.1.1) https://www.nist.gov/publications/guide-industrial-control-systems-ics-security	Center for Internet Security Critical Security Control 6: Access Control Management https://www.cisecurity.org/controls/access-control-management	Center for Internet Security Account Management/Access Control Standard (See Section 4.1.c, 4.2, & 4.3.c) https://www.cisecurity.org/wp-content/uploads/2020/06/Account-Management-Access-Control-Standard.docx CIS Information Security Policy (See Section 4.10.h to 4.10.k) https://www.cisecurity.org/controls/v8
Protect (PR)	2.F	Network Segmentation	ShadowServer https://www.shadowserver.org/what-we-do/network-reporting/	MITRE - ICS Network Segmentation https://attack.mitre.org/mitigations/M0930/ CISA - Layering Network Security Through Segmentation https://www.cisa.gov/resources-tools/resources/layering-network-security-through-segmentation-infographic	pfSense https://www.pfsense.org/getting-started/	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				NIST SP 800-41: Guidelines on Firewalls and Firewall (page 4-1 and 5-1) https://csrc.nist.gov/pubs/sp/800/41/r1/final NSA "Stop Malicious Cyber Activity Against Connected OT" Advisory https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF		
Protect (PR)	2.G	Detection of Unsuccessful (Automated) Login Attempts	None identified.	CIS Microsoft Windows 10 Stand-alone Benchmark (See pg. 50 and pg. 382) https://www.cisecurity.org/benchmark/microsoft_windows_desktop CISA's Weak Security Controls and Practices routinely Exploited for Initial Access https://www.cisa.gov/news-events/alerts/2022/05	None identified.	CIS Security Logging Standard Policy Template (See Appendix A) https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Logging-Standard.docx

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				/17/weak-security-controls-and-practices-routinely-exploited-initial CIS Password Policy Guide (See Section 5.1.6 & 5.1.7) https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide Microsoft Windows Security Policy Setting Reference https://learn.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/security-policy-settings-reference		
Protect (PR)	2.H	Phishing-Resistant Multifactor Authentication (MFA)	CISA Free Cybersecurity Services and Tools https://www.cisa.gov/resources-tools/resources/free-cybersecurity-services-and-tools	CIS Password Policy Guide (See Sections 2.1 & 6) https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide CISA Bad Practices https://www.cisa.gov/news-	None identified.	Identification and Authentication Policy (See Section 1 & Section 4.x) https://www.cisecurity.org/wp-content/uploads/2020/06/Identification-

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
			CISA Cybersecurity Resources for High-Risk Communities https://www.cisa.gov/audiences/high-risk-communities/cybersecurity-resources-high-risk-communities	events/news/bad-practices-0 CISA Implementing Phishing-Resistant MFA https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf CISA Security Tip: More than a Password https://www.cisa.gov/MFA Microsoft 365 Multi-Factor Authentication Reference https://learn.microsoft.com/en-us/microsoft-365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide		and-Authentication-Policy.docx
Protect (PR)	2.I	Basic Cybersecurity Training	None identified.	Cybersecurity Workforce Training Guide https://www.cisa.gov/resources-tools/resources/cyber	CISA Cybersecurity Training and Exercises https://www.cisa.gov/cybersecurity-training-exercises	CIS Security Awareness and Training Policy Security Awareness Skills Training Policy Template for CIS Control 14

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				security-workforce-training-guide FTC's Cybersecurity for Small Businesses https://www.ftc.gov/business-guidance/small-businesses/cybersecurity US Small Business Administration: Small Business Cybersecurity https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity	NICCS Federal Virtual Training Environment (FedVTE) https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte SANS Security Awareness Training https://www.sans.org/security-awareness-training/products/security-awareness-solutions/end-user/ [FEE-BASED] SANS Security Awareness Phishing Tools https://www.sans.org/security-awareness-training/products/security-awareness-solutions/phishing/ [FEE-BASED] SANS Security Awareness Engineer Training https://www.sans.org/security-awareness-training/products/specialized-training/ics-engineer/ [FEE-BASED]	https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.J	OT Cybersecurity Training	None identified.	CISA Cybersecurity Workforce Training Guide https://www.cisa.gov/resources-tools/resources/cybersecurity-workforce-training-guide US Small Business Administration: Small Business Cybersecurity https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity	ICS Training Available Through CISA https://www.cisa.gov/ics-training-available-through-cisa NICCS Federal Virtual Training Environment (FedVTE) Cybersecurity Training https://niccs.cisa.gov/education-training/federal-virtual-training-environment-fedvte SANS Hands-on ICS Training https://www.sans.org/cyber-security-courses/ics-scada-cyber-security-essentials/ [FEE-BASED]	
Protect (PR)	2.K	Strong and Agile Encryption	None identified.	Microsoft Core Infrastructure Guide - TLS https://learn.microsoft.com/en-us/mem/configmgr/core/plan-design/security/enable-tls-1-2	SSL/TSL How to Implement Transport Layer Security (TLS) https://www.ssl.com/guide/ssl-best-practices/	CIS Encryption Standard (See Sections 4.0 and 4.1) https://www.cisecurity.org/wp-content/uploads/2020/06/Encryption-Standard.docx SANS Acceptable Encryption Policy (See Section 4.3)

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
						https://www.sans.org/information-security-policy/
Protect (PR)	2.L	Secure Sensitive Data	None identified.	Microsoft Learn - Data Encryption at Rest https://learn.microsoft.com/en-us/dynamics365/business-central/dev-itpro/security/transparent-data-encryption Microsoft Support - How to encrypt a file https://www.microsoft.com/en-us/windows/learning-center/how-to-encrypt-file National Cybersecurity Alliance: Protect Data and Devices https://staysafeonline.org/cybersecurity-for-business/protect-data-and-devices/ Federal Trade Commission: A Guide for Business Protecting Personal Information https://www.ftc.gov/business-	Cyber Readiness Institute: The Cyber Readiness Program https://cyberreadinessinstitute.org/ KeePass Password Safe https://keepass.info/download.html	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				guidance/resources/protecting-personal-information-guide-business Microsoft Learn - Data Encryption at Rest https://learn.microsoft.com/en-us/azure/security/fundamentals/encryption-atrest Microsoft Support - How to encrypt a file https://www.microsoft.com/en-us/windows/learning-center/how-to-encrypt-file National Cybersecurity Alliance: Protect Data and Devices https://staysafeonline.org/cybersecurity-for-business/protect-data-and-devices/ Federal Trade Commission: A Guide for Business Protecting Personal Information https://www.ftc.gov/business-guidance/resources/pr		

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				otecting-personal-information-guide-business		
Protect (PR)	2.M	Email Security	None identified.	CISA Binding Operational Directive 18-01 - Enhance Email and Web Security https://www.cisa.gov/news-events/directives/bod-18-01-enhance-email-and-web-security FTC: Cybersecurity For Small Businesses https://www.ftc.gov/business-guidance/small-businesses/cybersecurity Global Cyber Alliance DMARC Setup Guide https://dmarcguide.globalcyberalliance.org/#/	None identified.	None identified.
Protect (PR)	2.N	Disable Macros by Default	None identified.	Microsoft Support: Enable or disable macros in Office for Mac https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-	None identified.	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				office-for-mac-c2494c99-a637-4ce6-9b82-e02cbb85cb96 Microsoft Support: Enable or disable macros in Microsoft 365 https://support.microsoft.com/en-us/office/enable-or-disable-macros-in-microsoft-365-files-12b036fd-d140-4e74-b45e-16fed1a7e5c6 CIS Intel Insight: How to Disable Macros https://www.cisecurity.org/insights/white-papers/intel-insight-how-to-disable-macros Microsoft: Macros Disabled By Default In Office https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked		
Protect (PR)	2.O	Document Device Configurations	None identified.	Center For Internet Security Benchmarks https://www.cisecurity.org/cis-benchmarks	CIS Hardware and Software Asset Tracking Spreadsheet https://www.cisecurit	CIS Configuration Management Policy (See Sections 1, 2, 5, & 8)

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
					y.org/insights/white-papers/cis-hardware-and-software-asset-tracking-spreadsheet	https://www.cisecurity.org/insights/white-papers/secure-configuration-management-for-cis-control-4 CIS Systems and Services Acquisition Policy (See Section 5) https://www.cisecurity.org/wp-content/uploads/2020/06/System-and-Services-Acquisition-Policy.docx
Protect (PR)	2.P	Document Network Topology	CIS Vulnerability Assessment https://www.cisecurity.org/services/vulnerability-assessments	DISA Sample Topology Diagram https://disa.mil/~/media/Files/DISA/Services/DISN-Connect/References/sample_les_topology.pdf Microsoft Support - Create a Basic Network Diagram https://support.microsoft.com/en-us/office/create-a-basic-network-diagram-f2020ce6-c20f-4342-84f7-bf4e7488843a	CISA CSET Tool https://www.cisa.gov/stopransomware/cyber-security-evaluation-tool-csetr Nmap: the Network Mapper - Free Security Scanner https://nmap.org/	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.Q	Hardware and Software Approval Process	None identified.	CISA Application Whitelisting for ICS https://www.cisa.gov/sites/default/files/documents/Guidelines%20for%20Application%20Whitelisting%20in%20Industrial%20Control%20Systems_S508C.pdf CISA Hardware Asset Management (HWAM) Capability https://www.cisa.gov/sites/default/files/cdm_files/Intro_to_HWAM.pdf Microsoft Learn-Software Center User Guide https://learn.microsoft.com/en-us/mem/configmgr/core/understand/software-center NIST SP 800-167 - Guide to Application Whitelisting https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-167.pdf	Security Scorecards GitHub - ossf/scorecard: OpenSSF Scorecard - Security health metrics for Open Source https://github.com/ossf/scorecard	SANS Software Installation Policy (See Sections 4.2 & 4.3) https://www.sans.org/information-security-policy/

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.R	System Backups	None identified.	NICCS Protecting Data from Ransomware and Other Data Loss Events https://www.nccoe.nist.gov/sites/default/files/legacy-files/msp-protecting-data-extended.pdf US Small Business Administration: Small Business Cybersecurity https://www.sba.gov/business-guide/manage-your-business/strengthen-your-cybersecurity	Microsoft - Backup and Restore in Windows https://support.microsoft.com/en-us/windows/back-up-your-windows-pc-87a81f8a-78fa-456e-b521-ac0560e32338 Google Backup & Sync https://support.google.com/drive/answer/7638428 https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt3cf8b9a0b2e45133/5e9ddb9ab1704560004196b5/disaster_recovery_plan_policy.pdf	CIS Contingency Planning Policy (see Sections 4 & 7) https://www.cisecurity.org/-/media/project/cisecurity/cisecurity/data/media/files/uploads/2020/06/Contingency-Planning-Policy.docx SANS Disaster Recovery Plan Policy (See Section 4.1) https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt3cf8b9a0b2e45133/5e9ddb9ab1704560004196b5/disaster_recovery_plan_policy.pdf
Protect (PR)	2.S	Incident Response (IR) Plans	None identified.	CISA Cybersecurity Incident Response https://www.cisa.gov/topics/cybersecurity-best-practices/organizations-and-cyber-safety/cybersecurity-incident-response	CISA Incident Response Training https://www.cisa.gov/resources-tools/programs/Incident-Response-Training CISA Tabletop Exercise Packages	CIS Cyber Incident Response Standard https://www.cisecurity.org/wp-content/uploads/2020/06/Cyber-Incident-Response-Standard.docx

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
					https://www.cisa.gov/cisa-tabletop-exercise-packages Cyber Readiness Institute: The Cyber Readiness Program https://cyberreadinessinstitute.org/ FCC Cybersecurity Planning Tool https://www.fcc.gov/cyberplanner	CIS Incident Response Policy https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17
Protect (PR)	2.T	Log Collection	CIS Managed Security Services (MSS) https://www.cisecurity.org/services/managed-security-services-mss [FEE-BASED]	Microsoft Learn - Windows Event Collector https://learn.microsoft.com/en-us/windows/win32/wec/windows-event-collector OMB 21-31 - Improving the Federal Government's Investigative and Remediation Capabilities Related to	Albert Network Monitoring and Management Specifically for SLTTs https://www.cisecurity.org/services/albert-network-monitoring [FEE-BASED] AT&T AlienVault OSSIM WebCast & White Paper https://cybersecurity.att.com/products/ossim	SANS Information Logging Standard Policy Document (See Sections 4.1, 4.2, & 4.4) https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt96697821fe4f2949/636f12dee3836b0c88e8f0a4/Information_Logging_Standard.pdf CIS Security Logging Standard Policy

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
				Cybersecurity Incidents https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf	pfSense Free Network Firewall Distribution https://www.pfsense.org/getting-started/	Document (See Section 4) https://www.cisecurity.org/wp-content/uploads/2020/06/Security-Logging-Standard.docx
Protect (PR)	2.U	Secure Log Storage	CIS Managed Security Services (MSS) https://www.cisecurity.org/services/managed-security-services-mss [FEE-BASED]	OMB 21-31 - Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf	AT&T AlienVault OSSIM https://cybersecurity.att.com/products/ossim	SANS Information Logging Standard (See Section 4.4) https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt96697821fe4f2949/636f12dee3836b0c88e8f0a4/Information_Logging_Standard.pdf CIS Security Logging Standard (See Section 4.4) https://www.cisecurity.org/wp-content/uploads/2020

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
						/06/Security-Logging-Standard.docx
Protect (PR)	2.V	Prohibit Connection of Unauthorized Devices	None identified.	Microsoft - Enabling and Disabling AutoRun https://learn.microsoft.com/en-us/windows/win32/shell/autoplay-reg INFOSEC - Physical security for ICS/SCADA environments https://resources.infosecinstitute.com/topics/scada-ics-security/physical-security-for-ics-scada-environments/ CISA - Risk of Portable Devices https://www.cisa.gov/uscert/sites/default/files/publications/RisksOfPortableDevices.pdf UK NCSC - Small Business Guide: Cybersecurity https://www.ncsc.gov.uk/collection/small-business-guide	Cyber Readiness Institute: The Cyber Readiness Program Free Cybersecurity Training for Businesses https://cyberreadinessinstitute.org	SANS Removable Media Policy (See Section 4) https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blta59236f183ab31b/5e9e06135352ae292603886c/removable_media_policy.pdf

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.W	No Exploitable Services on the Internet	CIS Penetration Testing https://www.cisecurity.org/services/penetration-testing [FEE-BASED] CIS Vulnerability Assessments https://www.cisecurity.org/services/vulnerability-assessments [FEE-BASED]	Center For Internet Security Benchmarks https://www.cisecurity.org/cis-benchmarks CISA Blog: Website Security https://www.cisa.gov/news-events/news/website-security CIS Exploited Protocols: RDP https://www.cisecurity.org/insights/blog/commonly-exploited-protocols-remote-desktop-protocol-rdp Stuff off Search https://www.cisa.gov/publication/stuff-off-search	Binary Edge https://app.binaryedge.io/sign-up CISA How-to Guide: Censys.io https://www.cisa.gov/sites/default/files/publications/Censys_Technical_508c.pdf CISA How-to Guide: Shodan https://www.cisa.gov/sites/default/files/publications/Shodan_Technical_508c.pdf	SANS Web Application Security Policy (see Section 4) https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt55091bed60041d8e/636d96f9cbd6b84ecb485eb3/Web_Application_Security_Policy.pdf

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Protect (PR)	2.X	Limit OT Connections to Public Internet	Managed Security Services (MSS) https://www.cisecurity.org/services/managed-security-services-mss [FEE-BASED]	CIS Password Policy Guide (See Sections 2.1, 6.1, & 6.2) https://www.cisecurity.org/insights/white-papers/cis-password-policy-guide Industrial Control Systems Cybersecurity Initiative https://www.cisa.gov/sites/default/files/publications/ICS-Monitoring-Technology-Considerations-Final-v2_508c.pdf Stuff off Search https://www.cisa.gov/publication/stuff-off-search	CISA How-to Guide: Censys.io https://www.cisa.gov/sites/default/files/publications/Censys_Technical_508c.pdf CISA How-to Guide: Shodan https://www.cisa.gov/sites/default/files/publications/Shodan_Technical_508c.pdf	None identified.
Detect (DE)	3.A	Detecting Relevant Threats and TTPs	None identified.	MITRE ATT&CK Groups https://attack.mitre.org/groups/ CISA Cybersecurity Alerts and Advisories https://www.cisa.gov/news-events/cybersecurity-advisories	Albert Network Monitoring https://www.cisecurity.org/services/albert-network-monitoring	None identified.

Category	ID	Security Practice	Advisory Support/Technical Assistance Service	Best Practice	Tool/Training	Policy Templates[41]
Respond (RS)	4.A	Incident Reporting	None identified.	US-CERT Federal Incident Notification Guidelines https://www.cisa.gov/federal-incident-notification-guidelines	CISA Incident Reporting Form https://us-cert.cisa.gov/forms/report	
Respond (RS)	4.B	Vulnerability Disclosure/Reporting	CIS Vulnerability Assessments https://www.cisecurity.org/services/vulnerability-assessments [FEE-BASED]	CISA Incident Reporting Form https://us-cert.cisa.gov/forms/report		CISA Vulnerability Disclosure Policy Template https://www.cisa.gov/vulnerability-disclosure-policy-template
Respond (RS)	4.C	Deploy Security.txt Files	None identified.	RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure https://www.rfc-editor.org/rfc/rfc9116	None identified.	Security.txt https://securitytxt.org/
Recover (RC)	5.A	Incident Planning and Preparedness	None identified.	CISA Emergency Services Sector Continuity Planning Suite https://www.cisa.gov/emergency-services-sector-continuity-planning-suite	None identified.	SANS Cyber Security Policy Templates https://www.sans.org/information-security-policy/