A city at night

Description automatically generated with low confidence

Cybersecurity Plan Template

High Risk

[January/2023]

# 

# Table of Contents

[Table of Contents 2](#_Toc127189903)

[Form Instructions 3](#_Toc127189904)

[Disclaimer 5](#_Toc127189905)

[About the Project 6](#_Toc127189906)

[Glossary of Terms 16](#_Toc127189907)

[Appendix 1 DOE Programs 21](#_Toc127189908)

[Appendix 2 Guidance and Standards 23](#_Toc127189909)

## Form Instructions

This cybersecurity plan template form (Template) is used by Infrastructure Investment and Jobs Act (IIJA) award selectees/selectee/recipients to create a detailed project Cybersecurity Plan (Plan). Section 40126 of the IIJA, also known as the Bipartisan Infrastructure Law (Pub. L. 117-58), authorizes the Secretary of Energy to require that certain projects funded under the law include a Plan. The Department of Energy (DOE or the Department) developed three Templates—one for high risk projects, one for medium risk projects, and one for low risk projects—to streamline the development and review of project Cybersecurity Plans. Each template includes space for important details that need to be considered, such as the goals, activities and milestones, timelines, and resources associated with the Plan. This ensures that nothing is forgotten and that the project cybersecurity runs smoothly.

This high risk Template helps project teams outline a plan of action for project cybersecurity. It also is a guide for project teams to follow when structuring a risk- appropriate Plan. The Template can be a helpful tool for project teams to create a comprehensive Plan to protect their project’s computer networks and systems. The benefits of using this Template include having a starting point for creating a Plan, ensuring that the essential elements are included, and having a guide on what needs to be in it. Project teams should create a manageable Plan that includes the elements in the categories in this Template.

To fill out this form, the project team will need to provide some basic information in their responses. Each category has a note that will help guide the response to the questions. Capitalized terms are defined in the Glossary, and CESER’s website has tools and resources that the project team may find useful when completing this template, including the DOE’s [Cybersecurity Capability Maturity Model (C2M2)](https://c2m2.doe.gov/C2M2%20Version%202.1%20June%202022.pdf).

Selectee/Recipients are encouraged to leverage existing DOE tools and resources and integrate them into their Plan. Appendix 1 contains links to some online tools and resources, including DOE programs Section 41026(b)(1) requires that the cybersecurity plan describe “plans to maintain cybersecurity between networks, systems, devices, applications, or components – (A) within the proposed solution of the project; and (B) at the necessary external interfaces at the proposed solution boundaries;”

Section 40126(b)(2) requires the cybersecurity plan to describe how the funding selectee/recipient will “will report known or suspected network or system compromises of the project to the Secretary;”

Section 40126(b)(4) requires the cybersecurity plan to describe how the funding selectee/recipient will “leverage applicable cybersecurity programs of the Department, including cyber vulnerability testing and security engineering evaluations.”

Section 40126(c)(1)(B) indicates that the selectee/recipient should “maximize the use of open guidance and standards, including, where possible, … -- (B) ) the Framework for Improving Critical Infrastructure Cybersecurity of the National Institute of Standards and Technology.

The Department recommends using open guidance and standards such as [the National Institute of Standards and Technology’s (NIST) Cybersecurity Framework (CSF)](https://www.nist.gov/cyberframework/framework) and the [C2M2 V2.1](https://c2m2.doe.gov/C2M2%20Version%202.1%20June%202022.pdf). This Cybersecurity Plan created pursuant to Section 40126 should document any deviation from open standards in responses in this template. The Selectee/recipient should also document where proprietary standards are utilized in responses in this template. Appendix 2 has links to useful guidance and standards that can help when designing the Plan.

The project team should not include Critical Energy Infrastructure Information (CEII) or other sensitive information, including personnel, confidential business, or procurement sensitive detail in its responses. If a project team believes that sensitive information is critical to the Plan’s review, they should notify the DOE Sponsoring Program Office before transmitting the plan to DOE so it can be managed with appropriate protections.

IIJA Selectees/recipients may be asked by the Sponsoring Program Office to complete this form after they are selected for an award but before the funding is issued. Creation of a Plan is an allowable project expense ONLY AFTER a project has been selected for funding and the Sponsoring Program Office has notified the project team that a Plan is required.

Work on a Plan before that time cannot be charged to the project’s Federal funds. Funding Selectees/recipients can obtain reimbursement for development of Plans completed after notification. DOE and its affiliate DOE lab partners will review the Plan and provide feedback to the Sponsoring Program Office, who may share that information with the Selectee/recipient.

Project teams should contact the DOE Sponsoring Program Offices for guidance on which template to complete and any related questions or concerns about the form.

The three templates and related material will be posted on [[Bipartisan Infrastructure Law Implementation | Department of Energy]](https://www.energy.gov/ceser/bipartisan-infrastructure-law-implementation).

## Disclaimer

Submission of a Cybersecurity Plan based on this form to DOE does not satisfy any regulatory or other requirement regarding cybersecurity planning, implementation, or reporting. The Selectee/recipient remains solely responsible for identifying and complying with all requirements imposed by other entities (including those pertaining to cybersecurity).

Neither the U.S. Government Submission nor any agency thereof, nor any of their employees nor its contractors, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the U.S. Government or any agency thereof.

The Secretary of Energy has determined that the release of information provided to or collected herein by the Federal Government as part of this cybersecurity plan, as described in Pub. L. 117-58 § 40126, 42 U.S.C. § 18725, (Cybersecurity Plan), could be detrimental to the physical security or cybersecurity of an electric utility or bulk-power system. Therefore, pursuant to Pub. L. 117-58 § 40126(e), such information shall be exempt from disclosure otherwise required by the Freedom of Information Act, as codified at 5 U.S.C. § 552. This exemption is limited to information provided to or collected by the Federal Government described in Pub. L. 117-58 § 41026, 42 U.S.C. §18725.

## About the Project

## Project Title:

## Sponsoring Program Office:

*Note: The project team will perform activities during the project period that outlined in the responses. After the project is over, the party responsible for the ongoing operation of the project will maintain the activities. Each response below includes a list of planned activities, a brief description of the project, key milestones, and associated dates.*

*The response to all the requests for information in the template should provide information include:*

*a brief, high-level response to the question and*

*key milestones (where applicable).*

## Asset, Change, and Configuration Management

Outline the plan to maintain an Asset Inventory and configuration management of the digital Assets and systems used in the project.

*Note: It is important to have an inventory of Assets for the project to manage risk. The inventory should include information on the Asset model number, software version number, Asset location, owner of the Asset, and priority of the Asset for the project. The Plan needs an effective configuration and change management process to avoid introducing Cybersecurity Vulnerabilities into the operating Cybersecurity Environment.*

*Change control applies to the entire project Asset lifecycle. Change control process steps usually include the following activities: requirements definition, testing, deployment, maintenance, and retirement from operation. The Cybersecurity Plan should provide a brief high-level description of the project’s Assets and Critical Assets and describe the high-level processes that will be followed to develop and maintain an Asset inventory, manage asset configuration, and provide change control.*

1. What is the project team’s plan to implement and maintain an Asset Inventory of its Information Technology (IT) Assets? *Provide a high-level description of the Plan and the project team’s commitment to develop and implement relevant policies and procedures.*
2. What is the project team’s plan to implement and maintain an Asset Inventory of its Operational Technology (OT) Assets? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
3. What is the project team’s plan to implement and maintain an inventory of its Information Assets? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
4. What is the project team’s plan to implement and maintain a process for IT Asset configuration and change management? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
5. What is the project team’s plan to implement and maintain a process for OT Asset configuration and change management? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
6. Which cybersecurity standards, guidelines, industry best practices, or guidance, etc. (if applicable) is the project team planning to use to support management of its digital Assets?
7. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing its IT and OT Assets? *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

## Threat and Vulnerability Management

Outline the plan to monitor Cybersecurity Threats and Cybersecurity Vulnerabilities in project digital systems and Assets.

*Note: Cybersecurity Threat (Threat) identification and response begins with collecting useful Threat information from reliable sources, interpreting that information, and responding to threats that can have the means, motive, and opportunity to affect the delivery of services.*

*Reducing Cybersecurity Vulnerabilities (Vulnerabilities) begins with collecting and analyzing Vulnerability information. Discovery of Vulnerabilities that could affect the delivery of services can include tools such as scanning tools, penetration tests, cybersecurity exercises, and audits. Analysis should include the potential effect of the vulnerability on exposed project Assets and Critical Assets, and the importance of the exposed asset in project cybersecurity. Vulnerabilities may be addressed by implementing mitigating controls, monitoring threat status, applying cybersecurity patches, replacing outdated equipment, or performing other activities.*

1. What is the project team’s plan to identify and address project Cybersecurity Vulnerabilities? *Provide a high-level description of the plan and the project team’s commitment to identify and address vulnerabilities.*
2. What is the project team’s plan to identify and address project Cybersecurity Threats? *Provide a high-level description of the plan and the project team’s commitment to identify and address threats.*
3. Which standards, guidelines, industry best practices, or guidance, etc. (if applicable) is the project team planning to use to support its management of Cybersecurity Threats and Vulnerabilities?
4. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing Cybersecurity Vulnerabilities and Cybersecurity Threats? *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

## Risk Management

Outline the plan to evaluate project Cybersecurity Risks and make Risk Management decisions.

*Note: Cybersecurity Risk (Cyber Risk) is defined as the possibility of harm or loss due to unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, or information assets. Managing project Cybersecurity Risk involves Risk Framing, identifying, and assessing risks, responding to risks (by accepting, avoiding, mitigating, and/or transferring risks), and monitoring risks over time. The use of a risk register—a list of risks and associated attributes—can help the process of Risk Management.*

1. What is the project team’s plan to establish and maintain a program for cyber risk assessment and management? *Provide a high-level description of the plan and the project team’s commitment to identify and address Cyber Risks.*
2. What is the project team’s plan to identify specific cyber risks? *Provide a high- level description of the plan to identify Cybers Risks?*
3. What is the project team’s plan for assessing Cyber Risks? *Provide a high-level description of the plan to assess Cyber Risks?*
4. What is the project team’s plan for addressing identified Cyber Risks? *Provide a high-level description of the plan to addressing Cyber Risks?*
5. Which standards, guidelines, industry best practices guidance, etc. (if applicable) is the project team planning to use to support its risk management program?
6. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing Cybersecurity Risks? *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

## Identity and Access Management

Outline the plan to limit access to systems and Assets used in the project

*Note: To protect project Assets, it is important that the Plan ensures access controls are in place. This includes limitations on logical and physical access to project data and Assets. Access control applies to individuals, devices, systems, and processes. This includes hardware, such as computer systems; software that runs on those systems that supply services like data storage; processes that involve people’s actions at work—like employees logging onto their accounts online before beginning work tasks each day. It also involves protecting information stored within a project network from external threats by using controls like encryption certificates. The project Plan should include maintaining identities, determining access requirements, granting access based on those requirements, and revoking access when it is no longer required. Improper access management practices can lead to unauthorized use, disclosure, destruction, or modification of project Assets.*

1. What is the project team’s plan to establish identities (for people and Assets) and manage authentication? *Provide a high-level description of the plan to establish identities and manage authentication.*
2. What is the project team’s plan to control logical access (e.g., electronic access) to the project’s key Assets and Critical Assets? *Provide a high-level description of the plan to control logical access.*
3. What is the project team’s plan to control physical access to the project’s key Assets and Critical Assets? *Provide a high-level description of the plan to control physical access.*
4. Which standards, guidelines, industry best practices guidance, etc. (if applicable) will the project team use to support its access management program?
5. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing access to Assets and Critical Assets? *Provide a high- level description of how resources, roles, and responsibilities will be managed.*

## Situational Awareness

Outline the plan to monitor the Cybersecurity Environment and maintain Situational Awareness.

*Note: Situational Awareness involves developing near-real-term knowledge of a dynamic operating environment. It’s the ability to perceive and comprehend how things are changing in your environment. It establishes and maintains activities and technologies, to collect, monitor, alarm, report, and use operational, security, and Threat information. The project team can establish Situational Awareness by monitoring the project’s IT, OT, and communication Assets. It is critical to know what other systems may be compromising or attacking yours. The project team can, for example, monitor and analyze data collected in logs to help understand the operational and cybersecurity status of project.*

1. What is the project team’s plan to perform logging activities for system processes and communication? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
2. What is the project team’s plan to perform monitoring of logging and other cybersecurity Situational Awareness information to identify potential Cybersecurity Events or Cybersecurity Incidents? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
3. What is the project team’s plan to establish and maintain an integrated picture of cybersecurity Situational Awareness? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
4. Which standards, guidelines, industry best practices guidance, etc. (if applicable) is the project team planning to use to support its Situation Awareness program?
5. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing Situational Awareness activities? *Provide a high- level description of how resources, roles, and responsibilities will be managed.*

## Event and Incident Response, Continuity of Operations

Outline the plan to respond to cybersecurity events and incidents.

*Note: The project team can mitigate the impact of Cybersecurity Events (Events) or Cybersecurity Incidents (Incidents) by preparing for them ahead of time. The project team should set up a plan to detect Events, including a process for reporting them, and outlining criteria for when a certain event is considered an Incident. The response plan helps the team appropriately deal with the aftermath of Events and Incidents. The incident response plan should include all phases of the Incident lifecycle—from triage, handling, communication, coordination, to recovery. Cybersecurity Events and Cybersecurity Incidents can also trigger external obligations like reporting to regulatory bodies.*

1. What is the project team’s plan to analyze Cybersecurity Events and declare Cybersecurity Incidents as warranted? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
2. What is the project team’s plan to respond to Cybersecurity Incidents? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
3. What is the project team’s plan to address cybersecurity in its program to maintain continuity of operations? *Provide a high-level description of the plan and the project team’s commitment to develop and implement relevant policies and procedures.*
4. Which standards, guidelines, industry best practices guidance, etc. (if applicable) are you planning to use to support your Cybersecurity Event and Cybersecurity Incident response program?
5. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing the program’s response to Cybersecurity Events and Incidents?

## Supply Chain and Third-Party Risk Management

Outline the plan to address Cybersecurity Supply Chain issues and Third- Party dependencies.

*Note: Without proper Third-Party Risk Management, the acquisition of products and services poses serious risks. Cybersecurity Supply Chain and Third-Party dependencies can expose project Assets to risks. The risks include acquiring software of unknown provenance, buying counterfeit (possibly malicious) hardware, and providing system access to external entities with inadequate security. Project teams can address this risk by exercising care when buying products and services, especially if they are from unknown sources that might not be safe. One way project teams address this risk is to supply specifications to their suppliers of systems, devices, and services to ensure they are secure and of good quality. Keep in mind that the cybersecurity characteristics of products and services vary widely.*

1. What is the project team’s plan to identify and manage Cybersecurity Risks associated with its Supply Chain? *Provide a high-level description of the plan and the project team’s commitment to manage the Cybersecurity Risks associated with the Supply Chain and Third Parties.*
2. What is the project team’s plan to identify and manage other Third-Party Cybersecurity Risks (e.g., partners, contractors, or service providers who have access to internal project data, systems, processes, or other privileged information)? *Provide a high-level description of the plan and the project team’s commitment to manage the Cybersecurity Risks associated with the Supply Chain and Third Parties.*
3. Which standards, guidelines, industry best practices guidance, etc. (if applicable) are you planning to use to support your management of Supply Chain and Third- Party program?
4. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing the Cybersecurity Risks associated with its program’s Supply Chain and risk involving Third Parties? *Provide a high-level description of how resources, roles, and responsibilities will be managed*

## Training

Outline the plan to prepare the project team to recognize and address cybersecurity issues.

*Note: Even if project team members have an education and experience in cybersecurity, they may need more training to be able to recognize cybersecurity issues as they come up. This is also true for service providers. Conducting periodic security awareness activities or exercises can help mitigate social engineering and other threats. The project team should evaluate the activities and exercises it performs to improve and update training. Additionally, vetting personnel through, for example, background checks and behavioral observation activities can also reduce Cybersecurity Risks.*

1. What is the project team’s plan to provide cybersecurity training for the project workforce? *Provide a high-level description of the plan and the project team’s commitment to provide cybersecurity and awareness activity for the project workforce.*
2. What is the project team’s plan to provide cybersecurity awareness activities for the project workforce? *Provide a high-level description of the plan and the project team’s commitment to provide cybersecurity and awareness activity for the project workforce.*
3. What is the project team’s plan to assign appropriate cybersecurity responsibilities to all members of the project team workforce? *Provide a high- level description of the plan and the project team’s commitment to provide cybersecurity and awareness activity for the project workforce.*
4. What is the project team’s plan to develop and retain appropriate cybersecurity capabilities in your project workforce? *Provide a high-level description of the plan and the project team’s commitment to provide cybersecurity and awareness activity for the project workforce.*
5. Which standards, guidelines, industry best practices guidance, etc. (if applicable) is the project team planning to use to support its project workforce management program?
6. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing the Cybersecurity Risks associated with its project’s workforce? *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

## Cybersecurity Architecture

Outline the plan to implement and maintain a secure project Cybersecurity Architecture.

Note: Establishing Cybersecurity Architecture involves identifying cybersecurity requirements for the project’s Assets and designing appropriate controls to protect them. Cybersecurity Architecture includes network design and protections, security, and data security. The effectiveness of the Cybersecurity Architecture is judged by how well the security controls work, individually and together, to achieve the desired level of project security.

1. What is the project team’s plan to implement appropriate network protections as an element of its project’s Cybersecurity Architecture? *Provide a high-level description of the plan and the Project team’s commitment to implement appropriate network protections.*
2. What is the project team’s plan to implement IT Asset security as an element of the Cybersecurity Architecture? *Provide a high-level description of the plan and the project team’s commitment to develop and implement software and data security.*
3. What is the project team’s plan to implement OT Asset security as an element of the Cybersecurity Architecture? *Provide a high-level description of the plan and the project team’s commitment to develop and implement software and data security.*
4. What is the project team’s plan to implement software security as an element of the Cybersecurity Architecture? *Provide a high-level description of the plan and the project team’s commitment to develop and implement software and data security.*
5. What is the project team’s plan to implement data security as an element of the Cybersecurity Architecture? *Provide a high-level description of the plan and the project team’s commitment to develop and implement software and data security.*
6. Which standards, guidelines, industry best practices guidance, etc. (if applicable) is the project team planning to use to support its Cybersecurity Architecture program?
7. What is the project team’s plan to assign proper resourcing, roles, and responsibilities for managing activities related to maintaining a secure Cybersecurity Architecture? *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

## Cybersecurity Program Management

Outline the plan to allocate resources and assign roles and responsibilities for Project cybersecurity management.

*Note: Cybersecurity management involves planning and implementing activities that meet project Cybersecurity Objectives. Those activities include setting up and overseeing a proper set of cybersecurity policies and procedures and organizing cybersecurity self- assessment activities.*

*Sponsorship is a key element in cybersecurity management, as the sponsor provides resources like people, tools, and funding to help with implementation. The role of the sponsor is essential to the success of a cybersecurity plan.*

1. What is the project team’s plan to manage the project's cybersecurity program? *Provide a high-level description of the plan for the overall management of the project’s cybersecurity program.*
2. What is the project team’s plan to establish and maintain an appropriate project cybersecurity management? *Provide a high-level description of the plan for the overall management of the project’s cybersecurity program.*
3. Which standards, guidelines, industry best practices guidance, etc. (if applicable) is the project team planning to use to support its management of the project’s cybersecurity.

What is the project team’s plan to assign proper resourcing, roles, and responsibilities for the management of cybersecurity? *Provide a high-level description of how resources, roles, and responsibilities will be managed.*

## Glossary of Terms

The Terms defined below guide IIJA Selectee/recipients in understanding and completing this cybersecurity plan template. The Terms are adapted from sources (e.g., the C2M2 Glossary, NIST Information Technology Laboratory Computer Security Resource Center Glossary) to align with the development of cybersecurity plans.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| **Assets** | For the purposes of this template, assets are hardware and software, as well as information essential to operating the project, including interconnected or interdependent business and technology systems and the environment in which they operate. (<https://c2m2.doe.gov/glossary#A>) |
| **Asset Inventory** | A list of assets including identification and location information. <https://csrc.nist.gov/glossary/term/inventory> |
| **Critical Assets** | Project assets that that if impacted by a cyber attack would have an immediate or severe on the Project. |
| **Cybersecurity Architecture** | An overarching Cybersecurity Plan for engineering and designing controls to protect a project’s Critical Assets controls can involve network design, network protections, application/software security, and data security. The Cybersecurity Architecture transcends point solutions for individual Assets, such as identity management or access control. |
| **Cybersecurity Environment** | Includes users, networks, devices, software, processes, stored or transit information, applications, services, and systems that can be directly or indirectly connected to networks and be impacted by a cyberattack |
| **Cybersecurity Event** | An anomalous occurrence in a system or network that may be an act or attempt, successful or unsuccessful, to gain unauthorized access to, disrupt or misuse related to a cybersecurity requirement. Depending on their potential impact, some events need to be declared as incidents. [(https://c2m2.doe.gov/glossary#E)](https://c2m2.doe.gov/glossary#E) |

|  |  |
| --- | --- |
| **Cybersecurity Incident** | An event, or series of events, that has the potential to significantly affect the project’s assets or the services the project provides and requires the project team to respond in to prevent or limit impact. Criteria for declaration of an incident are determined by the project team or its cybersecurity organization. [( https://c2m2.doe.gov/glossary#I)](https://c2m2.doe.gov/glossary#I) |
| **Cybersecurity Objectives** | Cybersecurity performance targets set by the project or organization. [(https://c2m2.doe.gov/glossary#O)](https://usdoe.sharepoint.com/sites/InfrastructureWorkingTeam-BIDImplementationandCoordinationTeams/Shared%20Documents/BID%20Implementation%20and%20Coordination%20Teams/10%20-%20Cybersecurity/Cybersecurity%20Plan/S%2040126%20Implementation/Materials%20for%20Oct%204%20Meeting/Cybersecurity%20Plan%20Templates/(https:/c2m2.doe.gov/glossary%23O)) |
| **Cybersecurity Plan** | IIJA Section 40126 defines the minimum criteria for project cybersecurity plans. |
| **Cybersecurity Program** | An integrated group of activities designed and managed to meet Cybersecurity Objectives for the project, an organization, or a key function. An existing organizational cybersecurity program can be applied or adapted to meet the needs of the Proposed Solution. [(https://c2m2.doe.gov/glossary#C)](https://c2m2.doe.gov/glossary#C) |
| **Cybersecurity Objective** | Cybersecurity performance targets set by the project or organization. [(https://c2m2.doe.gov/glossary#O)](https://c2m2.doe.gov/glossary#O) |
| **Cybersecurity Project Strategy** | In its simplest form, the cybersecurity project strategy is a list of cybersecurity objectives and a plan to meet them. For higher risk projects, the projectcybersecurity project strategy should be more comprehensive and include priorities, a governance approach, structure and organization for the project, and the sign off and oversight of senior management in the design of the cybersecurity project. |
| **Cybersecurity Risk** | The possibility of harm or loss due to unauthorized access, use, disclosure, disruption, modification, or destruction of IT, OT, or information assets. <https://c2m2.doe.gov/glossary#C> |
| **Cybersecurity Threats** | An action with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), resources, and other organizations through Information Technology (IT), Operational Technology (OT), or communications infrastructure via unauthorized access, destruction, disclosure, modification of information, or denial of service. [(https://c2m2.doe.gov/glossary#T)](https://c2m2.doe.gov/glossary#T) |
| **Cybersecurity Vulnerabilities** | A weakness or flaw in hardware, firmware, software, communications systems or devices, system procedures, internal controls, or implementation that could be exploited by a Cybersecurity Threat. ([https://c2m2.doe.gov/glossary#V](https://c2m2.doe.gov/glossary" \l "V)) |
| **Information Assets** | Information of value to the organization or project, such as business data, intellectual property, customer information, contracts, security logs, metadata, set points, and operational data, information assets may be in digital or non-digital form. <https://c2m2.doe.gov/glossary#I> |
| **Information Technology (IT)** | A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. This may include interconnected or interdependent business and technology systems and the environment in which they operate. <https://c2m2.doe.gov/glossary#I> |
| **Operational Technology (OT)** | Assets required for service delivery or production activities. Examples include industrial control systems, building management systems, fire control systems, process control systems, safety instrumented systems, Internet of Things (IoT) devices, and physical access control mechanisms. [( https://c2m2.doe.gov/glossary#O)](https://c2m2.doe.gov/glossary#O) |
| **Risk Framing** | The set of assumptions, constraints, risk tolerances, and priorities/trade-offs that shape an organization’s approach for managing risk. |
| **Risk Level** | For the purposed of this document, the following risk levels and their definitions will be used to.  Low Risk – Risks associated with the loss of confidentiality, integrity, or availability where all the credible scenarios do not exceed low impact. For example, the potential of a successful cyberattack to cause local impacts to systems and services but with no disruption on the local or regional electric system owing to backup systems or services that cannot be impacted by the same cyberattack. Another example is the loss of information that is not considered sensitive or does not have a substantial business or stakeholder impact.  Moderate Risk – Risks associated with the loss of confidentiality, integrity, or availability where there is at least one credible scenario that produces a medium impact, but there are no high impacts. For example, the potential of a successful cyberattack to cause local or more widespread regional disruptions in the electrical system but not impact the operation of the bulk electric system.  Another example is the loss of information that is considered sensitive (but not classified) or may have substantial business or stakeholder impacts.  High Risk – Risks associated with the loss of confidentiality, integrity, or availability where there is at least credible scenario with a high impact. For example, the potential of a successful cyberattack to result in impacts that affect the operation of the bulk electric system. Another example is the loss of information that is classified or of such a serious nature that it can be used to cause regional or national economic or stakeholder impacts. |
| **Risk Management** | An ongoing project’s process of identifying, analyzing, evaluating, and addressing a projects or an organization’s Cybersecurity Threats. Addressing cybersecurity actions involves prioritizing and adopting cybersecurity protections and related activities based on the cybersecurity threat’s potential adverse impact and likelihood. ([https://c2m2.doe.gov/glossary#R)](https://c2m2.doe.gov/glossary#R) |
| **Situation Awareness** | A sufficiently accurate and up-to-date understanding of the past, current, and projected future state of a system (including its cybersecurity status), in the context of the threat environment and risks to the system’s function, to support appropriate decision making. It involves the collection of data, such as via sensor networks, and data analysis (which may include modeling and simulation) to support automated or human decision making). Situational Awareness can involve tools that aid personnel in making decisions. Tools may include alarms or data analytics and visualization products. ([https://c2m2.doe.gov/glossary#S)](https://c2m2.doe.gov/glossary#S) |
| **Sponsoring Program Office** | The Department of Energy office awarding or dispersing the funding for the project. The office may be a DOE office or a state, local, tribal, or territorial office. |
| **Supply Chain** | A network of companies and people that participate in the production and delivery of a product or service. The supply chain system may start with the beginning stage of sourcing the raw materials to the final delivery of the product or service to end-users.  The supply chain lays out all aspects of the production process, including the activities involved at each stage, information that is being communicated, natural resources that are transformed into useful materials, human resources, and other components that go into the finished product or service.<https://c2m2.doe.gov/glossary#S> [https://csrc.nist.gov/glossary/term/supply\_chain)](https://csrc.nist.gov/glossary/term/supply_chain) |
| **Third-Party Risk Management** | The C2M2 domain with the purpose to establish and maintain controls to manage the cyber risks arising from suppliers and other third parties, commensurate with the risk to critical infrastructure and organizational objectives. |

## Appendix 1 DOE Programs

The list below contains DOE resources that can be leveraged to create project cybersecurity plans.

|  |  |  |
| --- | --- | --- |
| **Reference or Program** | **Description** | **Website** |
| Cybersecurity Capability Maturity Model (C2M2) | A widely adopted maturity model for the electric sector. May inform high TRL projects resulting in deployment and operation of technology with the highest potentially beneficial cybersecurity priorities. | C2M2 Version 2.1 June 2022 (energy.gov) |
| Cyber- Informed Engineering (CIE) | May guide low TRL project teams to engineer out cyber risk, thus reducing the potential attack surface  of developed technologies. | <https://www.energy.gov/sites/default/files/2022-06/FINAL%20DOE%20National%20CIE%20Strategy%20-%20June%202022_0.pdf> |
| Consequence- Driven Cyber- Informed Engineering (CCE) | May aid organizations that are employing developed technologies to develop mitigations to ensure that critical functions are immune to cyber sabotage. | <https://inl.gov/cce/> |
| Cybersecurity for the Operational Technology Environment  (CyOTE™) | May help organizations create a holistic sensing strategy to detect adversary techniques. affecting developed technologies. | [Cybersecurity for the Operational Technology Environment (CyOTE) | Department of Energy](https://www.energy.gov/ceser/cybersecurity-operational-technology-environment-cyote) |
| CyberStrike | Information about cyberattacks on energy infrastructure, including mitigation strategies. | [https://inl.gov/wp- content/uploads/2021/07/21- 50064\_CyberstrikeFlyer.pdf](https://inl.gov/wp-%20content/uploads/2021/07/21-%2050064_CyberstrikeFlyer.pdf) |
| Cyber Testing for Resilient Industrial Control | Used for vulnerability testing. | <https://inl.gov/cytrics/> |
| Distributed Energy Resources Cybersecurity Framework (DERCF) | Can help indicate cybersecurity priorities for projects focus on deployment and operation of devices and subsystems that are part of distributed energy resource systems (DERs). | <https://dercf.nrel.gov/> |
| Distributed Energy Resources Risk Manager (DER- RM) | Supports DER compliance with the NIST Risk Management Framework. | PowerPoint: [https://www.nist.gov/system/files/ documents/2021/02/22/Day1.7- Anuj%20-%20DER-](http://www.nist.gov/system/files/)  [RM\_NIST%20presentation.pdf](http://www.nist.gov/system/files/) |
| *Energy Sector Cybersecurity Framework Implementation Guidance* | *Framework Implementation Guidance* specifically for energy sector owners and operators. | [Energy Sector Cybersecurity Framework Implementation Guidance](https://www.energy.gov/ceser/articles/energy-sector-cybersecurity-framework-implementation-guidance) |

## Appendix 2 Guidance and Standards

These third-party resources may be useful when structuring and implementing cybersecurity plans. The list below is not comprehensive.

|  |  |  |
| --- | --- | --- |
| **Resource** | **Description** | **Website** |
| Cybersecurity & Infrastructure Security Agency (CISA) | CISA’s Shields Up campaign provides alerts and technical guidance to help organizations take proactive steps to protect against active cyber threats. | [https://www.cisa.gov/shields-up](http://www.cisa.gov/shields-up) |
| CISA  Free Cybersecurity Services and Tools | This repository includes cybersecurity services provided by CISA, widely used open-source tools, and free tools and services offered by private and public sector organizations across the cybersecurity community. | [Free Cybersecurity Services and Tools | CISFA](https://www.cisa.gov/free-cybersecurity-services-and-tools) |
| CISA | ICS-related alerts, advisories, and reports. | [https://www.cisa.gov/uscert/ics](http://www.cisa.gov/uscert/ics) |
| Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) –  Industrial Control Systems |  |  |
| CISA  The Cyber Security Evaluation Tool (CSET) | The Cyber Security Evaluation Tool (CSET) provides a systematic, disciplined, and repeatable approach for evaluating an organization’s security posture. | [CSET Download (inl.gov)](https://cset-download.inl.gov/) |
| NIST  *Framework for Improving Critical Infrastructure Cybersecurity* | This publication describes a voluntary risk management framework (“the Framework”) that consists of standards, guidelines, and best practices to manage cybersecurity-related risk.  The Framework’s prioritized, flexible, and cost-effective approach helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security. | [https://www.nist.gov/publications/](http://www.nist.gov/publications/) framework-improving-critical- infrastructure-cybersecurity-version-11 |
| National Rural Electric Cooperative Association (NRECA) | This document is useful for cooperatives developing a cybersecurity plan for general business purposes. It does not address any specific current or potential regulations. | [guide-cybersecurity-mitigation-plan.pdf (cooperative.com)](https://www.cooperative.com/programs-services/bts/documents/guide-cybersecurity-mitigation-plan.pdf)  *DOE Award No: DE-OE0000222* |