NIST Voting Technology Series
NIST VTS 200-1

Cybersecurity Framework Election Infrastructure Profile

Mary Brady
Gema Howell
Joshua M. Franklin
Christina Sames
M. Schneider
Julie Snyder
David Weitzel

This publication is available free of charge from:
https://doi.org/10.6028/NIST.VTS.200-1

NATIONAL INSTITUTE OF
STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Voting Technology Series
NIST VTS 200-1

Cybersecurity Framework Election Infrastructure Profile

Mary Brady*
Software Systems Division
Information Technology Laboratory
**Former NIST employee; all work for this publication was done while at NIST.*

Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Joshua M. Franklin
The Turnout, LLC

Christina Sames
M. Schneider
Julie Snyder
David Weitzel
The MITRE Corporation

This publication is available free of charge from:
https://doi.org/10.6028/NIST.VTS.200-1

January 2024

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on 2024-01-23

How to Cite this NIST Technical Series Publication

Brady M, Howell G, Franklin J, Sames C, Schneider M, Snyder J, Weitzel D (2023) Cybersecurity Framework Election Infrastructure Profile. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Voting Technology Series (VTS) NIST VTS 200-1. https://doi.org/10.6028/NIST.VTS.200-1

NIST Author ORCID iDs

Gema Howell: 0000-0002-0428-5045

Contact Information

voting@nist.gov

Abstract

This document is a Cybersecurity Framework Profile developed for voting equipment and information systems that support elections. This Election Infrastructure Profile can be utilized by election administrators and IT professionals who manage election infrastructure to reduce the risks associated with these systems. This Profile provides a voluntary, risk-based approach for managing cybersecurity activities and reducing cyber risk to election infrastructure. This Profile is meant to supplement but not replace current cybersecurity standards and industry guidelines that election administrators are already leveraging.

Keywords

Cybersecurity Framework; Election Infrastructure Profile; elections; risk management; security controls; voter registration; voting; voting systems.

Acknowledgments

In the development of this specification, the authors recognize the significant contributions made by individuals and organizations involved in both election administration and in developing and deploying election technology. This includes public and private sectors, whose thoughtful and constructive comments improved the overall quality, thoroughness, and usefulness of this publication. The authors gratefully acknowledge and appreciate the following contributors for their keen and insightful assistance with developing this specification (all contributions were done while at the listed affiliations):

- Chris Wlaschin, Election Systems & Software (ES&S)
- Benjamin Long, NIST
- Maurice Turner, Center for Democracy and Technology (CDT)
- Michael South, Amazon

The authors also wish to thank the participants of the August 27–28, 2019, workshop to develop a Cybersecurity Framework Election Infrastructure Profile, including participants from the Election Infrastructure Subsector[1] (EIS) Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC),[2] as well as other stakeholders.

[1] The EIS is a subsector of the Government Facilities Sector.

[2] For Election Infrastructure charters and membership details, refer to the Department of Homeland Security website, which was published on May 8, 2019, and accessed on September 25, 2019.

Table of Contents

List of Tables

Introduction

The NIST Cybersecurity Framework (also referred to simply as “the Framework”) is a voluntary, risk-based assemblage of industry standards and best practices that are designed to help organizations manage cybersecurity risks [1]. The Framework was created through collaboration between industry, academia, and government, and it uses a common language to address and manage cybersecurity risks in a cost-effective way based on business needs without imposing additional regulatory requirements. The Framework is designated to be customized to address specific risks to an organization, and many sectors have opted to create their own prioritization of the Framework, known as a Profile. Elections are no different, as government officials charged with the conduct of elections have their own metrics for success, priorities, and threat profiles. Election infrastructure may come under cyberattack or be subject to natural disasters, and the appropriate defenses and contingencies should be identified and tailored to the subsector’s needs.

Purpose

This Election Infrastructure Profile (referred to as “Profile” from here forward) was developed to broadly consider the entire election infrastructure and engage with election stakeholders to understand their mission objectives (MO) and priorities. This Profile leverages NIST Cybersecurity Framework V 1.1. With any risk management process or when making cybersecurity decisions, an organization must consider their own specific needs. This Profile demonstrates one aspect of how cybersecurity activities can be prioritized based on election-specific mission objectives.

This Profile can be used in several ways:

- To highlight high-priority security expectations and the prioritization of security activities,
- To perform a self-assessment comparison of current risk management and security practices, or
- As a baseline or example Profile to reference when developing a Profile (or Target Profile).

Scope

In 2017, the Department of Homeland Security (DHS) designated election systems as critical infrastructure and established Election Infrastructure as a subsector of the Government Facilities Sector. It is one of 16 critical infrastructure sectors identified in *Presidential Decision Directive 21 (PDD-21): Critical Infrastructure Security and Resilience*, whose assets, systems, and networks are considered so vital to the Nation that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health and safety, or any combination thereof [2]. This Profile describes election infrastructure systems, including voting equipment and information systems that support elections (see *Overview of Election Infrastructure*). This Profile is not intended to cover every aspect of information technology (IT) used within elections nor every use case. The Profile is meant to engender risk-based cybersecurity decisions for a certain subset of election infrastructure using specific mission objectives identified by the community. Best practices for cybersecurity provided by organizations charged with responsibilities related to elections, such as DHS’s Cybersecurity & Infrastructure Security Agency (CISA) and Election Assistance Commission (EAC), should still be utilized.

Audience

The intended audience for this document includes election officials, manufacturers and developers of voting systems, and service providers and consultants who work with and support elections and voting systems. Others in the election community, including the general public, may also find this material to be a valuable reference for understanding the security activities and priorities of election infrastructure. Election processes are complex, so some background in election administration and technology is useful for understanding the material in this specification. Knowledge of cybersecurity concepts is also helpful.

Using This Document

This Profile of election infrastructure was developed through consensus by a group of election stakeholders. Since its assessments are necessarily broad, it can and should be modified to fit specific uses. This may include updating the definitions and rankings of mission objectives or revising the Category and Subcategory scores (see *Summary Framework Category Prioritization*) to suit specific missions, systems, and processes. While this Profile may be useful as a reference, it should not supersede users' expertise and needs.

Document Structure

The remainder of this document is organized into the following sections and appendices:

- *Overview of Election Infrastructure* discusses the types of information systems used for elections and to support voting activities.
- *Overview of the Cybersecurity Framework* discusses the main elements of the Framework, what defines a Framework Profile, and how it all relates to this Profile.
- *Profile Development Methodology* describes the methodology used to develop this Profile.
- *Election Infrastructure Mission Objectives (MO)* describes the Mission Objectives, which are the granular outcomes that support the mission of the Election Infrastructure subsector.
- *Summary Framework Category Prioritization* summarizes the Categories selected for this Profile.
- *Priority Subcategories by Mission Objective* details specific prioritization for Subcategories for the Election Infrastructure subsector.

The document also contains the following supporting material:

- References list the sources used in the development of this publication.
- Appendix A: Acronyms lists selected acronyms and abbreviations used in this publication.
- Appendix B: Workshop Attendees lists the attendees of the Election Infrastructure Profile workshop.
- Appendix C: Informative References provides a framework of informative references.

Overview of Election Infrastructure

As previously stated, the Election Infrastructure subsector was created in 2017 under the Government Facilities Sector [2]. Figure 1 was created by the Cybersecurity and Infrastructure Security Agency (CISA) and identifies the components of the election process that are included in election infrastructure.

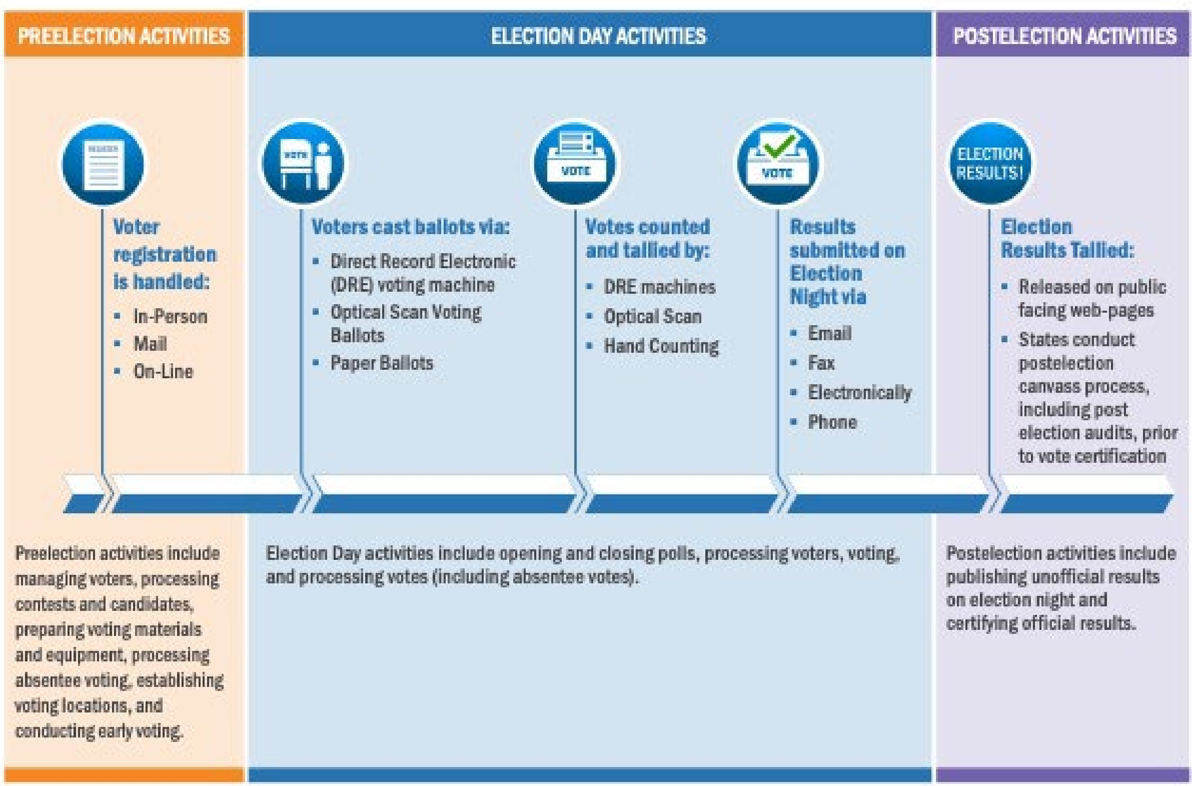
PREELECTION ACTIVITIES
ELECTION DAY ACTIVITIES
POSTELECTION ACTIVITIES
REGISTER
VOTE
VOTE
VOTE
ELECTION RESULTS!
Voter registration is handled:
In-Person
Mail
On-Line
Voters cast ballots via:
Direct Record Electronic (DRE) voting machine
Optical Scan Voting Ballots
Paper Ballots
Votes counted and tallied by:
DRE machines
Optical Scan
Hand Counting
Results submitted on Election Night via
Email
Fax
Electronically
Phone
Election Results Tallied:
Released on public facing web-pages
States conduct postelection canvass process, including post election audits, prior to vote certification
Preelection activities include managing voters, processing contests and candidates, preparing voting materials and equipment, processing absentee voting, establishing voting locations, and conducting early voting.
Election Day activities include opening and closing polls, processing voters, voting, and processing votes (including absentee votes).
Postelection activities include publishing unofficial results on election night and certifying official results.

Figure 1. U.S. electoral process infographic [3]

Exploring the Election Infrastructure Subsector

The Election Infrastructure (EI) Subsector is comprised of individuals and organizations who build, manage, and maintain a diverse set of systems, networks, and processes that must function together to conduct elections. The following types of systems fall under the definition of election infrastructure [4]:

- *Voter registration databases*: These databases store the list of citizens who are eligible to vote and often include personally identifiable information (PII) that can be used to determine where a voter votes and authenticate them to a poll worker. Voter registration databases may have an internet-facing web application that allows voters to register and validate their information online.
- *Voting machines*: Also known as voting systems, these devices enable voters to cast their ballots. These machines may use touchscreens, optical scans, or a hybrid voting system. They may or may not be certified by state or federal authorities to a standard, such as the Voluntary Voting System Guidelines (VVSG) [5].

- *IT infrastructure and systems used to manage elections (e.g., counting, auditing, and displaying election results and post-election reporting to certify and validate result*s): These can include a variety of election-oriented IT systems, such as electronic pollbooks, central count optical scan devices, election management systems, and software used to run audits. These devices may be certified by state or federal authorities to a standard, such as the Voluntary Voting System Guidelines (VVSG) [5].
- *Storage facilities for election and voting system infrastructure*: These are commonly government facilities but may also include schools, churches, and other venues.
- *Polling places, including early voting locations and other voting infrastructure*: These are the physical locations where U.S. citizens cast their votes, including vote centers and ballot drop boxes.

This Profile follows CISA's definition for election infrastructure and excludes political action committees, campaigns, and any other non-state or local government election-related groups.

Relationship to the Voluntary Voting System Guidelines (VVSG)

The 2002 Help America Vote Act (HAVA) [6] mandated that the U.S. Election Assistance Commission (EAC) set and maintain the VVSG, which are requirements that allow voting systems to be tested against the Federal Government's voting system testing and certification process [5]. These requirements range from general election functionality (e.g., supporting various types of ballot logic and multiple languages) to cybersecurity and human factor needs, as well as granular requirements that specific implementations of voting systems can be tested against. While the scope of the VVSG relates to the portion of the Profile that discusses voting machines*,* this Profile covers many other systems. The Profile does not supersede the VVSG, as each document fulfills a different need within government and industry.

Overview of the Cybersecurity Framework

The NIST Cybersecurity Framework [1] assists organizations in managing and reducing cybersecurity risks in a way that responds to unique needs, risks, threats, requirements, or the cybersecurity sophistication of an organization. Providing a common language for understanding, managing, and expressing cybersecurity risks fosters communication among internal and external stakeholders and across an organization, regardless of cybersecurity expertise.

The Framework consists of three main components: the Core, Profiles, and Implementation Tiers. The Core is a catalog of desired cybersecurity activities and outcomes using a common language that is easy to understand. A Framework Profile is an alignment of organizational requirements, objectives, risk appetite, and resources with the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving an organization's cybersecurity. The Implementation Tiers help organizations consider the appropriate level of rigor for their cybersecurity program and are often used as a communication tool to discuss risk appetite, mission priority, and budget.[3]

The Framework Core

The Framework presents industry standards, guidelines, and practices in a manner that allows cybersecurity activities and outcomes to be expressed to all levels of an organization, from the executive level to individuals with operational job roles. The Framework Core consists of five concurrent and continuous Functions that provide a strategic view of an organization’s cybersecurity posture:

1. **Identify** — Develop organizational understanding to manage cybersecurity risks to systems, assets, data, and capabilities. The activities in the Identify Function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs. Examples of outcome Categories within this Function include Asset Management, Business Environment, Governance, Risk Assessment, and Risk Management Strategy.

2. **Protect** — Develop and implement the appropriate safeguards to ensure the delivery of critical infrastructure services. The activities in the Protect Function support the ability to limit or contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include Access Control, Awareness and Training, Data Security, Information Protection Processes and Procedures, Maintenance, and Protective Technology.

3. **Detect** — Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event. The activities in the Detect Function enable the timely discovery of cybersecurity events. Examples of outcome Categories within this Function include Anomalies and Events, Security Continuous Monitoring, and Detection Processes.

4. **Respond** — Develop and implement the appropriate activities to take action after a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact

[3] For the purposes of this Profile, further discussion on Implementation Tiers is not included.

of a potential cybersecurity event. Examples of outcome Categories within this Function include Response Planning, Communications, Analysis, Mitigation, and Improvements.

5. **Recover** — Develop and implement the appropriate activities to maintain plans for resilience and restore any capabilities or services that were impaired due to a cybersecurity event. The activities in the Recover Function support timely recovery to normal operations to reduce the impact of a cybersecurity event. Examples of outcome Categories within this Function include Recovery Planning, Improvements, and Communications.

The Core also identifies Categories and Subcategories[4] for each Function and matches them with example Informative References (i.e., existing standards, guidelines, and practices) to provide context for the development of Framework Profiles and Mission Objectives. Table 1 shows the 23 Categories spread across the Functions.

Table 1. Framework Functions and Categories

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

[4] Categories represent discrete cybersecurity outcomes, while Subcategories represent specific outcomes of technical and/or management activities to support the Category.

Framework Profiles

A Framework Profile (or “Profile”) represents a prioritization of outcomes based on but not limited to the business needs, regulatory requirements, resources, and risk tolerance that an organization has selected from the Framework Categories and Subcategories. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a particular implementation scenario.

Profiles can be used to identify opportunities for improving cybersecurity posture by comparing a Current Profile (i.e., the “as is” state) with a Target Profile (i.e., the “to be” state). They also offer a consistent way for organizations to discuss cybersecurity objectives across organizational roles using common terminology. Individuals within the organization may use the Profile to prioritize the allocation of resources to cybersecurity improvements or areas of particular concern. This Election Infrastructure Profile should serve as a reference for those involved in election infrastructure. To obtain Current and Target Profiles, an organization may begin with this Profile and update it to fit their circumstances. The goal of this document is not to prescribe security standards but to ease the process for organizations to set their own goals.

The development of a Profile starts with the identification of an organization’s mission objectives, which are high-level goals that must be achieved in order for the organization to succeed at its primary mission. The mission objectives provide the necessary context for an organization to manage its cybersecurity risk as it relates to a specific mission need. Categories and Subcategories that are especially relevant to each mission objective are then identified and prioritized to fit the needs of the organization. Individuals within the organization may use the Profile to prioritize the allocation of resources to cybersecurity improvements.

Profile Development Methodology

This section discusses the approach used to create this Profile and the workshops held to identify relevant mission objectives.

Profile Workshop

In August of 2019, the National Institute of Standards and Technology (NIST) conducted a workshop to gather stakeholder input on the development of a Profile for Election Infrastructure in the United States. The workshop included participants from the Election Infrastructure Subsector[5] (EIS) Government Coordinating Council (GCC), the Sector Coordinating Council (SCC) [7], and other stakeholders. The workshop consisted of sessions with the following activities:

- Defining the mission objectives for election infrastructure in the United States, as formulated by the workshop participants. Mission objectives represent the fundamental, specific outcomes that support the mission of the election infrastructure.
- Identifying the relative importance of each mission objective to the overall success and integrity of the election process, as prioritized by the workshop participants. These operational priorities were then used to inform security priorities.
- Identifying and ranking the top three Framework Categories (out of the 23 shown in Table 1) for each mission objective that participants consider to be most important for securely accomplishing that objective, as well as additional Categories that are considered important for that objective.

Follow-On Working Sessions Profile Development

The final step in the methodology was the development of this Profile, which provides the results of the workshop, follow-on working sessions with stakeholders, and post-workshop analysis.[6] The aggregated ranking from the initial workshop enabled a post-workshop analysis to define a prioritization of Categories that were considered moderate, moderate-possibly-high, and high priority (see *Summary Framework Category Prioritization*) and was used to facilitate the subsequent ranking of the most important cybersecurity Subcategories (out of a total of 108) for each mission objective (see *Priority Subcategories by Mission Objective*).

[5] The EIS is a subsector of the Government Facilities Sector.

[6] This included a public comment period for this document that ended on May 14, 2021.

Election Infrastructure Mission Objectives (MO)

Table 2 shows the 10 mission objectives and their relative priorities based on stakeholder ratings at the NIST workshop.

Table 2. Election infrastructure mission objectives

Priority	*Mission Objective*
1	Conduct and Oversee Voting Period Activities†
2	Prepare and Maintain Election Systems†
3	Process and Maintain Voter Registration†
4	Prepare for a Specific Election†
5	Perform Ongoing Election Administration Functions
6	Conduct Audits
7	Conduct Election "Wrap-Up" Activities
8	Manage Crisis/Strategic Communications
9	Oversee Office Administration
10	Maintain Workforce

† Identifies the highest priority (or "top") mission objectives

A description of each mission objective follows, including bullet points that convey a preliminary understanding of relevant activities and the rationale for top mission objectives. When developing a Profile, these mission objectives and their definitions can be updated to better address the specific aspects of an organization (e.g., election jurisdiction).

1. **Conduct and Oversee Voting Period Activities.**† This mission objective encompasses all activities that are directly associated with the election *during the time when voters can submit their votes and when election officials can receive voted ballots.* This mission objective includes all voting period activities that are required to allow for *remote voting (e.g., absentee, mailed, military, overseas)*, *in-person early voting*, *election day voting*, *and provisional ballot voting*. During the working sessions, Mission Objective 1 was bifurcated into two phases:

   - Phase **1A** addresses activities associated with vote capture, such as early voting, election day voting, and absentee/mailed voting.

   - Phase **1B** addresses activities associated with vote aggregation, tabulation, canvassing, recounting (as necessary), and enumeration through the certification and reporting of election results.

   The discussion revealed that the process and people involved (e.g., voters, poll workers, election officials) in each phase created a greater distinction between what happens in Mission Objective 1A versus Mission Objective 1B.

Some activities that are relevant to this mission objective include:

- Open and close polls
- Set up voting system within the polling place
- Vote and submit ballots
- Check-in voters and determine eligibility
- Send ballots by mail/electronically
- Report on election night
- Aggregate, tabulate, canvas, recount (as necessary), and enumerate votes
- Transmit/send tabulation results to central tabulation center/back office
- Certify and publish election results

Rationale: This mission objective represents "game day" activities, as articulated by numerous workshop participants, and is fundamental to a free and fair election process.

2. **Prepare and Maintain Election Systems.**† This mission objective encompasses all aspects of preparing and maintaining the systems used for elections, including systems that connect to the backend (e.g., e-poll books) and all other election systems (e.g., voting systems).[7] This involves a holistic approach to the processes and procedures for acquiring, testing, certifying, configuring, and protecting election systems. Some activities that are relevant to this mission objective include:

   - Procure voting systems and supplies (e.g., keyboards, monitors, mice).
   - Test and certify election systems
   - Update election systems
   - Store election systems in a secure location

   Rationale: This mission objective represents essential precursor activities that are critical to Mission Objective 1.

3. **Process and Maintain Voter Registration.**† This mission objective encompasses all aspects of data and systems that are associated with voter registration, specifically processing voter registration data/information, ensuring the privacy and security of voter information, and maintaining the systems associated with those processes. This mission objective represents *an ongoing process* that includes election day registration, where allowed. Some activities that are relevant to this mission objective include:

   - Maintain voter registration list/database
   - Maintain voter registration website

[7] Voter registration systems and backend services, such as email, are discussed in separate mission objectives.

- Process voter registrations
- Release information to third parties, as allowed or required by law

Rationale: This mission objective represents critical activities for protecting the integrity of voter information and ensuring that eligible citizens can properly vote. Failing to achieve this mission objective could have significant impacts on public trust and confidence in current and future election outcomes.

4. **Prepare for a Specific Election.**† This mission objective encompasses the activities that need to take place to prepare for a specific election. Every election is different and requires distinct preparation, from the ballot style to the selection of the polling places. Some activities that are relevant to this mission objective include:

    - Establish voting locations (e.g., polling places, vote centers)
    - Transport and store equipment, ballots, and other necessary materials to voting locations
    - Process candidate filings and contests
    - Prepare voting materials (e.g., ballots)
        - Define ballot design/definition
        - Print ballots
        - Publish sample ballots
    - Maintain geographical data (e.g., addresses, precinct boundaries, precinct alternatives)

    Rationale: This mission objective represents essential precursor activities that are critical to Mission Objective 1.

5. **Perform Ongoing Election Administration Functions.** This mission objective encompasses the administrative functions that are necessary for day-to-day operations ***exclusively related to elections***. Some activities that are relevant to this mission objective include:

    - Acquire election-related tools and applications
    - Hire staff and acquire support services/contracts
    - Practice data hygiene
    - Manage chain of custody
    - Monitor and comply with applicable laws and policies
    - Preserve election records

6. **Conduct Audits.** This mission objective encompasses all audits in every phase of the process. There are various types of audits that can be categorized under three high-level categories: *quality audit*, *security audit*, *and tabulation audit*. Some activities that are relevant to this mission objective include:

    - *Security Audits*

    - Security audit of voting systems prior to election day
    - Security audit of voting systems on election day
    - Compliance audit
    - Chain-of-custody audit
- *Tabulation Audits*
    - Hand-count audit
    - Risk-limiting audit
    - Ballot comparison audit
- *Quality Audits*
    - Logic and accuracy audit
    - Ballot content audit
    - Public test (i.e., mock election) — audit prior to initial voting
    - Parallel test — run an extra voting machine in the polling place to validate results

7. **Conduct Election "Wrap-Up" Activities.** This mission objective encompasses everything that needs to be done after election results are certified and published (i.e., the tasks necessary to officially close out the election). Some activities that are relevant to this mission objective include:
    - Retain and secure election materials
    - Check voting equipment
    - Pay fees and reimburse polling locations
    - Bill districts for services
    - Communicate post-election lessons learned
8. **Manage Crisis/Strategic Communications.** This mission objective encompasses the timing, content, and conduct of communications with government and election officials (e.g., the Governor and Secretary of State), security and law enforcement (e.g., DHS, FBI), the press, and the public during and after events that impact or appear to impact the conduct of a free and fair election. Some activities that are relevant to this mission objective include:
    - Update and manage social media accounts
    - Process Freedom of Information Act (FOIA) requests
    - Respond to natural disasters or other unexpected events
    - Interact with election observers
    - Report vulnerabilities/cyberattacks

9. **Oversee Office Administration.** This mission objective encompasses *back office, non-election-specific information technology* and the general support services necessary for day-to-day operations. These include tools and applications, such as email, internal and contracted support services, and IT supply chain management. Some activities that are relevant to this mission objective include:

    - Support email system
    - Support other general services
    - Support the state systems necessary for elections (e.g., Motor Vehicle Administration [MVA] records)

10. **Maintain Workforce.** This mission objective encompasses the functions associated with effectively acquiring, training, and leading essential personnel to conduct free and fair elections. Elections employ one of the largest temporary workforces in the Nation. Some activities that are relevant to this mission objective include:

    - Provide training
    - Adopt and regularly reinforce processes and procedures
    - Recruit poll workers for specific elections
    - Pay and reimburse poll workers
    - Protect election and poll workers’ sensitive information
    - Mitigate insider threats

Summary Framework Category Prioritization

The stakeholders identified and ranked the top Category from each of the five Functions that they considered to be the most important for securely achieving each mission objective. For the purposes of interpreting and sharing these preliminary results, the Categories were weighted based on the numerical and high scores and ranked according to the following criteria:

- **High Priority (H):** Based on the number of votes per Category and how close those votes were to ranking a Category as most important (i.e., rank 1) in terms of securely achieving the mission objective (i.e., ≥3.0 votes and ≤ 2.0 average rank OR ≥ 5.0 votes and ≤ 2.5 average rank)
- **Moderate-Possibly-High Priority (M-H):** Possibly high priority due to the number of votes and score (i.e., ≥5.0 votes and ≤ 3.0 average OR ≥3.0 votes and ≤ 2.0 average)
- **Moderate Priority (M):** Received one or more votes, indicating a degree of importance over those that were not selected at all

Priority Categories by Mission Objective

Tables 3 through 12 show the Category prioritization for the 10 high-level mission objectives described in *Election Infrastructure Mission Objectives (MO)*.

Table 3. Conduct and Oversee Voting Period Activities (MO 1A and 1B)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	Asset Management (ID.AM) Governance (ID.GV)	Risk Assessment (ID.RA)	N/A
PROTECT	Awareness and Training (PR.AT)	Access Control (PR.AC) Information Protection Processes & Procedures (PR.IP)	N/A
DETECT	N/A	N/A	N/A
RESPOND	N/A	N/A	N/A
RECOVER	N/A	N/A	N/A

Table 4. Prepare and Maintain Election Systems (MO 2)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	Asset Management (ID.AM)	N/A	N/A
PROTECT	Access Control (PR.AC)	N/A	N/A
DETECT	N/A	Detection Processes (DE.DP)	Security Continuous Monitoring (DE.CM)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
RESPOND	N/A	Response Planning (RS.RP) Mitigation (RS.MI)	N/A
RECOVER	N/A	N/A	Recovery Planning (RC.RP)

Table 5. Process and Maintain Voter Registration (MO 3)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	N/A	N/A	N/A
PROTECT	Access Control (PR.AC) Data Security (PR.DS)	N/A	N/A
DETECT	N/A	Anomalies and Events (DE.AE)	N/A
RESPOND	N/A	N/A	Response Planning (RS.RP)
RECOVER	N/A	N/A	Recovery Planning (RC.RP)

Table 6. Prepare for a Specific Election (MO 4)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	Asset Management (ID.AM)	Governance (ID.GV)	N/A
PROTECT	N/A	Awareness and Training (PR.AT) Information Protection Processes & Procedures (PR.IP)	N/A
DETECT	N/A	Anomalies and Events (DE.AE)	N/A
RESPOND	N/A	N/A	N/A
RECOVER	N/A	Recovery Planning (RC.RP)	N/A

Table 7. Perform Ongoing Election Administration Functions (MO 5)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	Business Environment (ID.BE) Governance (ID.GV)	N/A	N/A

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
PROTECT	N/A	Awareness and Training (PR.AT) Data Security (PR.DS)	N/A
DETECT	N/A	N/A	N/A
RESPOND	N/A	N/A	Response Planning (RS.RP)
RECOVER	N/A	Recovery Planning (RC.RP)	Improvements (RC.IM)

Table 8. Conduct Audits (MO 6)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	N/A	Asset Management (ID.AM)	N/A
PROTECT	N/A	Access Control (PR.AC)	N/A
DETECT	Anomalies and Events (DE.AE)	N/A	N/A
RESPOND	N/A	N/A	N/A
RECOVER	N/A	N/A	N/A

Table 9. Conduct Election “Wrap-Up” (Previously “Post-Election”) Activities (MO 7)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	Asset Management (ID.AM) Governance (ID.GV)	N/A	N/A
PROTECT	N/A	Information Protection Processes & Procedures (PR.IP) Protective Technology (PR.PT)	N/A
DETECT	N/A	Anomalies and Events (DE.AE)	N/A
RESPOND	N/A	N/A	N/A
RECOVER	N/A	N/A	Recovery Planning (RC.RP)

Table 10. Manage Crisis/Strategic Communications (MO 8)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	N/A	N/A	Governance (ID.GV)
PROTECT	N/A	N/A	Information Protection Processes & Procedures (PR.IP)
DETECT	N/A	N/A	Anomalies and Events (DE.AE)
RESPOND	Response Planning (RS.RP) Communications (RS.CO)	N/A	N/A
RECOVER	N/A	Communications (RC.CO)	N/A

Table 11. Oversee Office Administration (MO 9)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	Asset Management (ID.AM)	Supply Chain Risk Management (ID.SC)	N/A
PROTECT	N/A	Access Control (PR.AC) Awareness and Training (PR.AT)	N/A
DETECT	N/A	Anomalies and Events (DE.AE)	Security Continuous Monitoring (DE.CM)
RESPOND	N/A	N/A	N/A
RECOVER	N/A	N/A	Recovery Planning (RC.RP)

Table 12. Maintain Workforce (MO 10)

Function	High Priority	Moderate-Possibly-High Priority	Moderate Priority
IDENTIFY	N/A	Asset Management (ID.AM) Business Environment (ID.BE)	N/A
PROTECT	Awareness and Training (PR.AT)	Access Control (PR.AC) Data Security (PR.DS)	N/A
DETECT	N/A	N/A	Anomalies and Events (DE.AE)
RESPOND	N/A	N/A	N/A
RECOVER	N/A	N/A	Recovery Planning (RC.RP)

Summary Table

Table 13 provides a summary view of Framework Category prioritization that was derived from stakeholder scoring to compare similarities and differences across all mission objectives. Initial observations and items under consideration include:

- Strong emphasis on Identify and Protect across all mission objectives
- Strong emphasis on several Categories across several mission objectives, particularly:
    - Asset Management (ID.AM)
    - Governance (ID.GV)
    - Access Control (PR.AC)
    - Awareness and Training (PR.AT)
    - Anomalies and Events (DE.AE)
    - Recovery Planning (RC.RP)

Table 13. Summary table of mission objective Categories

Categories	**1a**	**1b**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
IDENTIFY											
Asset Management (ID.AM)	H	H	H		H		M-H	H		H	M-H
Business Environment (ID.BE)						H					M-H
Governance (ID.GV)	H	H			M-H	H		H	M		
Risk Assessment (ID.RA)	M-H	M-H									
Risk Management Strategy (ID.RM)											
Supply Chain Risk Management (ID.SC)										M-H	
PROTECT											
Access Control (PR.AC)			H	H			M-H			M-H	M-H
Awareness and Training (PR.AT)	H	H			M-H	M-H				M-H	H
Data Security (PR.DS)				H		M-H					M-H
Information Protection Processes & Procedures (PR.IP)	M-H	M-H			M-H			M-H	M		
Maintenance (PR.MA)											
Protective Technology (PR.PT)								M-H			
DETECT											
Anomalies and Events (DE.AE)				M-H	M-H		H	M-H	M	M-H	M
Security Continuous Monitoring (DE.CM)			M							M	

Categories	**1a**	**1b**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
Detection Processes (DE.DP)			M-H								
RESPOND											
Response Planning (RS.RP)			M-H	M		M			H		
Communications (RS.CO)									H		
Analysis (RS.AN)											
Mitigation (RS.MI)			M-H								
Improvements (RS.IM)											
RECOVER											
Recovery Planning (RC.RP)			M	M	M-H	M-H		M		M	M
Improvements (RC.IM)						M					
Communications (RC.CO)									M-H		

Priority Subcategories by Mission Objective

This section provides an example of how an election stakeholder may prioritize their approach to addressing the Subcategories. Each election jurisdiction may have different priorities when making cybersecurity decisions. As with Mission Objective and Category rankings, users should adjust the priorities to meet their unique needs.

This Profile summaries of priority Subcategories in Tables 14 through 36 can be used in several ways, including:

- To highlight high-priority security expectations and the prioritization of security activities
- To perform a self-assessment comparison of current risk management and security practices
- As a baseline or example Profile to reference when developing a Current Profile or Target Profile

The initial Category rankings informed the level of priority given to the Subcategories (i.e., outcomes-based activities). For each mission objective, only the Subcategories of those Categories that had been identified as moderate, moderate-possibly-high, or high priority were considered for elevation above average criticality. The following “dot” charts indicate the results. Note that all Subcategories contain at least one dot, indicating that all Subcategories are relevant to mission objective security. The presence of multiple dots is meant to indicate Subcategories that merit more urgent focus, with three dots considered to be the most urgent and two dots considered to be less so. Each of these Subcategories were ranked to determine whether it was considered to be of high (●●●), moderate (●●), or average (●) urgency for securely achieving the mission objective. To assist with addressing the Subcategories, Appendix C lists informative references that are aligned with each Subcategory.

Table 14. Asset Management (ID.AM) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	●●●	●●●	●●●	●	●●●	●	●●●	●●●	●	●	●●
		ID.AM-2: Software platforms and applications within the organization are inventoried.	●●	●●	●●●	●	●●●	●	●●●	●●●	●	●●●	●
		ID.AM-3: Organizational communication and data flows are mapped.	●●●	●●●	●	●	●	●	●	●	●	●	●
		ID.AM-4: External information systems are catalogued.	●●●	●●●	●	●	●	●	●●●	●	●	●●●	●
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	●●●	●●●	●●●	●	●●	●	●	●●●	●	●	●●●
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	●●	●●	●●●	●	●●	●	●●	●●	●	●●	●●●

Table 15. Business Environment (ID.BE) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
IDENTIFY (ID)	**Business Environment (ID.BE):** The organization's mission, objectives, stakeholders, and activities are understood and prioritized. This information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated.	●	●	●	●	●	●	●	●	●	●	●
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated.	●	●	●	●	●	●	●	●	●	●	●
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	●	●	●	●	●	●●	●	●	●	●	●●●
		ID.BE-4: Dependencies and critical functions for the delivery of critical services are established.	●	●	●	●	●	●●●	●	●	●	●	●●
		ID.BE-5: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	●	●	●	●	●	●●●	●	●	●	●	●●●

Table 16. Governance (ID.GV) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
IDENTIFY (ID)	**Governance (ID.GV):** The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information cybersecurity policy is established and communicated.	●	●	●	●	●●	●●	●	●●	●	●	●
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	●	●	●	●	●●●	●●	●●	●●	●	●	●
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	●●●	●●●	●	●	●●●	●●●	●●●	●●●	●	●	●
		ID.GV-4: Governance and risk management processes address cybersecurity risks.	●	●	●	●	●	●	●●●	●●	●	●	●

Table 17. Risk Assessment (ID.RA) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
IDENTIFY (ID)	**Risk Assessment (ID.RA):** The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	●	●	●	●	●	●	●	●	●●●	●	●
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	●●●	●●●	●	●	●	●	●	●	●●	●	●
		ID.RA-3: Threats, both internal and external, are identified and documented.	●	●	●	●	●	●	●	●	●	●	●
		ID.RA-4: Potential business impacts and likelihoods are identified.	●●	●●	●	●	●	●	●	●	●●●	●	●
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	●●●	●●●	●	●	●	●	●	●	●	●	●
		ID.RA-6: Risk responses are identified and prioritized.	●	●	●	●	●	●	●	●	●	●	●

Table 18. Risk Management Strategy (ID.RM) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
IDENTIFY (ID)	**Risk Management Strategy (ID.RM):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	●	●	●	●	●	●	●	●	●	●	●
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	●	●	●	●	●	●	●	●	●	●	●
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	●	●	●	●	●	●	●	●	●	●	●

Table 19. Supply Chain Risk Management (ID.SC) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
IDENTIFY (ID)	**Supply Chain Risk Management (ID.SC):** The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risks. The organization has established and implemented the processes to identify, assess, and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	●	●	●	●	●	●	●	●	●	●●	●
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	●	●	●	●	●	●	●	●	●	●●	●
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	●	●	●	●	●	●	●	●	●	●●●	●

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm that they are meeting their contractual obligations.	●	●	●	●	●	●	●	●	●	●●	●
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	●	●	●	●	●	●	●	●	●	●●●	●

Table 20. Access Control (PR.AC) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
PROTECT (PR)	**Access Control (PR.AC):** Access to assets and associated facilities is limited to authorized users, processes, devices, activities, and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices users and processes.	●●	●●	●●●	●●	●	●	●	●	●	●●	●●●
		PR.AC-2: Physical access to assets is managed and protected.	●●●	●●●	●●●	●●●	●	●	●	●	●	●●●	●●
		PR.AC-3: Remote access is managed.	●●	●●●	●●●	●●●	●	●	●	●	●	●●●	●●
		PR.AC-4: Access permissions and authorizations are managed and incorporate the principles of least privilege and separation of duties.	●●	●●	●●●	●●●	●	●	●	●	●	●●●	●●●
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	●●	●●●	●●	●●●	●	●	●	●	●	●●	●
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	●	●	●●●	●●	●	●	●	●	●	●	●●●

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks).	●●●	●●●	●●●	●●●	●	●	●	●	●	●	●●●

Table 21. Awareness and Training (PR.AT) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
PROTECT (PR)	**Awareness and Training (PR.AT):** The organization’s personnel and partners are given cybersecurity awareness education and adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained.	●●	●●	●	●	●	●●	●	●	●	●●●	●●●
		PR.AT-2: Privileged users understand their roles and responsibilities.	●●●	●●●	●	●	●●●	●●●	●	●	●	●●●	●●●
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	●	●●●	●	●	●●	●●	●	●	●	●●	●●
		PR.AT-4: Senior executives understand their roles and responsibilities.	●	●	●	●	●●	●	●	●	●	●	●
		PR.AT-5: Physical and information security personnel understand their roles and responsibilities.	●●●	●●●	●	●	●●●	●●●	●	●	●	●	●

Table 22. Data Security (PR.DS) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
PROTECT (PR)	**Data Security (PR.DS):** Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data at rest is protected.	●	●	●	●●●	●	●●●	●●	●	●	●	●●
		PR.DS-2: Data in transit is protected.	●	●	●	●●●	●	●●●	●●	●	●	●	●●
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	●	●	●	●	●	●●●	●●●	●	●	●	●●●
		PR.DS-4: Adequate capacity to ensure availability is maintained.	●	●	●	●●●	●	●	●●	●	●	●	●●
		PR.DS-5: Protections against data leaks are implemented.	●	●	●	●●	●	●●	●	●	●	●	●●●
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	●	●	●	●●●	●	●●	●●●	●	●	●	●
		PR.DS-7: The development and testing environments are separate from the production environment.	●	●	●	●●	●	●	●	●	●	●	●
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	●	●	●	●●	●	●	●●●	●	●	●	●

Table 23. Information Protection Processes and Procedures (PR.IP) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
PROTECT (PR)	**Information Protection Processes and Procedures (PR.IP):** Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained to incorporate security principles (e.g., concept of least functionality).	●	●	●	●	●●●	●	●	●●	●	●	●
		PR.IP-2: A system development life cycle to manage systems is implemented.	●	●	●	●	●	●	●	●	●	●	●
		PR.IP-3: Configuration change control processes are in place.	●●	●●	●	●	●●	●	●	●	●	●	●
		PR.IP-4: Backups of information are conducted, maintained, and tested.	●●	●●	●	●	●●●	●	●	●●●	●	●	●
		PR.IP-5: Policies and regulations regarding the physical operating environment for organizational assets are met.	●●●	●●●	●	●	●●●	●	●	●●	●	●	●
		PR.IP-6: Data is destroyed according to policy.	●●●	●●●	●	●	●	●	●	●●	●	●	●
		PR.IP-7: Protection processes are improved.	●	●	●	●	●	●	●	●	●	●	●

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
		PR.IP-8: The effectiveness of protection technologies is shared.	●	●	●	●	●●	●	●	●	●●●	●	●
		PR.IP-9: Response plans (i.e., incident response and business continuity) and recovery plans (i.e., incident recovery and disaster recovery) are in place and managed.	●●●	●●●	●	●	●	●	●	●●	●●●	●	●
		PR.IP-10: Response and recovery plans are tested.	●	●	●	●	●	●	●	●	●●●	●	●
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	●	●	●	●	●	●	●	●●	●	●	●
		PR.IP-12: A vulnerability management plan is developed and implemented.	●	●	●	●	●	●	●	●	●●	●	●

Table 24. Maintenance (PR.MA) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
PROTECT (PR)	**Maintenance (PR.MA):** Industrial control and information system components are maintained and repaired consistent with policies and procedures.	**PR.MA-1:** The maintenance and repair of organizational assets are performed and logged in a timely manner with approved and controlled tools.	●	●	●	●	●	●	●	●	●	●	●
		PR.MA-2: The remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	●	●	●	●	●	●	●	●	●	●	●

Table 25. Protective Technology (PR.PT) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
PROTECT (PR)	**Protective Technology (PR.PT):** Technical security solutions are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	●	●	●	●	●	●	●	●●	●	●	●
		PR.PT-2: Removable media is protected and its use restricted according to policy.	●	●	●	●	●	●	●	●●	●	●	●
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	●	●	●	●	●	●	●	●	●	●	●
		PR.PT-4: Communications and control networks are protected.	●	●	●	●	●	●	●	●	●	●	●
		PR.PT-5: Mechanisms (e.g., fail-safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	●	●	●	●	●	●	●	●	●	●	●

Table 26. Anomalies and Events (DE.AE) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner, and the potential impacts of events are understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	●	●	●	●●	●●●	●	●	●	●	●●●	●
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	●	●	●	●●●	●●●	●	●●	●●●	●	●	●
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	●	●	●	●	●	●	●●●	●●	●	●●	●
		DE.AE-4: The impacts of events are determined.	●	●	●	●●●	●	●	●●●	●●	●●●	●●	●
		DE.AE-5: Incident alert thresholds are established.	●	●	●	●●●	●	●	●●●	●●	●●	●●●	●

Table 27. Security Continuous Monitoring (DE.CM) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
DETECT (DE)	**Security Continuous Monitoring (DE.CM):** Information systems and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	●	●	●	●●●	●	●	●	●	●	●●●	●
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	●	●	●	●●●	●	●	●	●	●	●●	●
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	●	●	●	●●●	●	●	●	●	●	●	●
		DE.CM-4: Malicious code is detected.	●	●	●	●●●	●	●	●	●	●	●●●	●
		DE.CM-5: Unauthorized mobile code is detected.	●	●	●	●	●	●	●	●	●	●	●
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	●	●	●	●●●	●	●	●	●	●	●	●
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	●	●	●	●●●	●	●	●	●	●	●●●	●
		DE.CM-8: Vulnerability scans are performed.	●	●	●	●●●	●	●	●	●	●	●●●	●

Table 28. Detection Processes (DE.DP) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
DETECT (DE)	**Detection Processes (DE.DP):** Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well-defined to ensure accountability.	●	●	●●	●	●	●	●	●	●	●	●
		DE.DP-2: Detection activities comply with all applicable requirements.	●	●	●●●	●	●	●	●	●	●	●	●
		DE.DP-3: Detection processes are tested.	●	●	●●●	●	●	●	●	●	●	●	●
		DE.DP-4: Event detection information is communicated.	●	●	●●	●	●	●	●	●	●	●	●
		DE.DP-5: Detection processes are continuously improved.	●	●	●●	●	●	●	●	●	●	●	●

Table 29. Response Planning (RS.RP) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained to ensure timely response to detected cybersecurity events.	**RS.RP-1:** The response plan is executed during or after an event.	●	●	●	●●●	●	●●●	●	●	●●●	●	●

Table 30. Communications (RS.CO) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RESPOND (RS)	**Communications (RS.CO):** Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and the order of operations when a response is needed.	●	●	●	●	●	●	●	●	●●●	●	●
		RS.CO-2: Incidents are reported consistent with established criteria.	●	●	●	●	●	●	●	●	●	●	●
		RS.CO-3: Information is shared consistent with response plans.	●	●	●	●	●	●	●	●	●●	●	●
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	●	●	●	●	●	●	●	●	●●●	●	●
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	●	●	●	●	●	●	●	●	●●	●	●

Table 31. Analysis (RS.AN) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RESPOND (RS)	**Analysis (RS.AN):** Analysis is conducted to ensure adequate responses and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated.	●	●	●	●	●	●	●	●	●	●	●
		RS.AN-2: The impact of an incident is understood.	●	●	●	●	●	●	●	●	●	●	●
		RS.AN-3: Forensics are performed.	●	●	●	●	●	●	●	●	●	●	●
		RS.AN-4: Incidents are categorized consistent with response plans.	●	●	●	●	●	●	●	●	●	●	●
		RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	●	●	●	●	●	●	●	●	●	●	●

Table 32. Mitigation (RS.MI) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
RESPOND (RS)	**Mitigation (RS.MI):** Activities are performed to prevent the expansion of an event, mitigate its effects, and eradicate the incident.	**RS.MI-1:** Incidents are contained.	●	●	●●●	●	●	●	●	●	●	●	●
		RS.MI-2: Incidents are mitigated.	●	●	●●●	●	●	●	●	●	●	●	●
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	●	●	●●●	●	●	●	●	●	●	●	●

Table 33. Improvements (RS.IM) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RESPOND (RS)	**Improvements (RS.IM):** Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned.	●	●	●	●	●	●	●	●	●	●	●
		RS.IM-2: Response strategies are updated.	●	●	●	●	●	●	●	●	●	●	●

Table 34. Recovery Planning (RC.RP) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure the timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** The recovery plan is executed during or after a cybersecurity incident.	●●●	●●●	●●	●●●	●●●	●●●	●●●	●●●	●	●●●	●●●

Table 35. Improvements (RC.IM) Subcategories

			Mission Objectives										
Function	**Category**	**Subcategory**	**1A**	**1B**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
RECOVER (RC)	**Improvements (RC.IM):** Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned.	●	●	●	●	●	●	●	●	●	●	●
		RC.IM-2: Recovery strategies are updated.	●	●	●	●	●	●	●	●	●	●	●

Table 36. Communications (RC.CO) Subcategories

			Mission Objectives										
Function	Category	Subcategory	1A	1B	2	3	4	5	6	7	8	9	10
RECOVER (RC)	**Communications (RC.CO):** Restoration activities are coordinated with internal and external parties, such as coordinating centers, internet service providers, owners of attacking systems, victims, other CSIRTs, and vendors.	**RC.CO-1:** Public relations are managed.	●	●	●	●	●	●	●	●	●●	●	●
		RC.CO-2: Reputation after an event is repaired.	●	●	●	●	●	●	●	●	●	●	●
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders and executive and management teams.	●	●	●	●	●	●	●	●	●●●	●	●

References

[1] National Institute of Standards and Technology (2018) Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. (National Institute of Standards and Technology, Gaithersburg, MD). https://doi.org/10.6028/NIST.CSWP.04162018

[2] Cybersecurity and Infrastructure Security Agency (2019) *CISA - Cyber+Infrastructure*. Available at https://www.dhs.gov/cisa/critical-infrastructure-sectors

[3] Cybersecurity and Infrastructure Security Agency *U.S. Electoral Process Infographic*, Available at https://www.cisa.gov/sites/default/files/publications/18_0301_nppd_electoral-process-graphic.pdf

[4] U.S. Department of Homeland Security (2023) *Election Security*. Available at https://www.dhs.gov/topic/election-security

[5] U.S. Election Assistance Commission (2023) Voluntary Voting System Guidelines Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

[6] Help America Vote Act of 2002, H.R. 3295 (2023) Available at https://www.eac.gov/sites/default/files/eac_assets/1/6/HAVA41.PDF

[7] Cybersecurity and Infrastructure Security Agency (2019) *Government Facilities Sector—Election Infrastructure Subsector: Charters and Membership*. Available at https://www.cisa.gov/government-facilities-election-infrastructure-charters-and-membership

Appendix A: Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

AC
Access Control

AE
Anomalies and Events

AM
Asset Management

AN
Analysis

AT
Awareness and Training

BE
Business Environment

CM
Security Continuous Monitoring

CO
Communications

DE
Detect

DP
Detection Processes

DS
Data Security

EI
Election Infrastructure

EIS
Election Infrastructure Subsector

GCC
Government Coordinating Council

GV
Governance

ID
Identity

IM
Improvements

IP
Information Protection Processes and Procedures

MA
Maintenance

MI
Mitigation

MO
Mission Objective

PDD
Presidential Decision Directive

PII
Personally Identifiable Information

PR
Protect

PT
Protective Technology

RA
Risk Assessment

RC
Recover

RP
Recovery Planning

RP
Response Planning

RM
Risk Management Strategy

RS
Respond

SaaS
Software as a Service

SC
Supply Chain Risk Management

SCC
Sector Coordinating Council

SSP
Sector-Specific Plan

VVSG
Voluntary Voting System Guidelines

Appendix B: Workshop Attendees

This is an alphabetically ordered list of those who registered to attend the Profile Workshop that was held from August 27–28, 2019.

Table 37. Profile Workshop attendees

No.	Last Name	First Name	Organization
1	Adkins	Christina Worrell	Texas Secretary of State
2	Aumayr	Paul	EAC
3	Bowers	Jessica	EAC
4	Cohen	Amy Lauren	National Association of State Election Directors
5	Davenport	Daniel	Virginia Department of Elections
6	Figueroa	Juan	DHS
7	Forson	Lindsey Marie	National Association of Secretaries of State
8	Franklin	Josh	Center for Internet Security
9	Frye	Felicia	The MITRE Corporation
10	Gookin	Eric	Office of the Secretary of State of Iowa
11	Hancock	Brian	Unisyn Voting Solutions
12	Harris	Jonathan Michael	VR Systems Inc
13	Hirsch	Bernie	MicroVote
14	King	Jonathan Bradley	Agency Office of the Secretary of State of Indiana Election Division
15	Lichtenheld	Peter James	Hart InterCivic
16	Lowan	Daniel	The MITRE Corporation
17	Macias	Ryan Stephen	Lafayette Group – on behalf of CISA
18	Martin-Rozumitowicz	Beata	IFES
19	Merrick	Joel	Office of the Secretary of State of Iowa
20	Munro	George Alexander	Bpro, Inc.
21	Newby	Brian	EAC
22	Nichols	David	Virginia Department of Elections
23	Patrick	Tammy Lynn	Democracy Fund
24	Peterson	Jesse Russell Antone	SLI compliance
25	Reynolds	Leslie D.	National Association of Secretaries of State
26	Sames	Christina A	The MITRE Corporation
27	Sawhey	Nimit	Voatz
28	Smith	James E.	DHS/CISA/EI SSA
29	Snyder	Julie, Nethery	NIST NCCoE/MITRE
30	South	Michael	Amazon Web Services
31	Suver	James Richard	Runbeck Election Services, Inc.
32	Tatum	Cliff	EAC

No.	Last Name	First Name	Organization
33	Turner	Maurice Rafael	Center for Democracy and Technology
34	Twumasi-Ankrah	Afua Amoanima	Clear Ballot
35	Ward	Paul	The MITRE Corporation
36	Wlaschin	Chris	ES&S

Appendix C: Informative References

Below is a replicated list of the informative references from *Framework for Improving Critical Infrastructure Cybersecurity* [1]. This list can be used as supporting material when considering how to address or meet the subcategory activities.

Table 38. Informative References from *Framework for Improving Critical Infrastructure Cybersecurity*[8]

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM)**	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 5** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried.	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 5** CM-8
		ID.AM-3: Organizational communication and data flows are mapped.	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 5** AC-4, CA-3, CA-9, PL-8, SA-17
		ID.AM-4: External information systems are catalogued.	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 5** AC-20, PM-5, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value.	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1

[8] A complete and up to date list of informative references can be found using Cybersecurity and Privacy Reference Tool at https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_1_1_0/home

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev. 5** CP-2, RA-2, RA-9, SA-20, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established.	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 5** CP-2, PS-7, PM-2, PM-29
	Business Environment (ID.BE)	**ID.BE-1:** The organization's role in the supply chain is identified and communicated.	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 5** SR-1, SR-3
		ID.BE-2: The organization's place in critical infrastructure and its industry sector are identified and communicated.	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 5** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated.	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 5** PM-11
		ID.BE-4: Dependencies and critical functions for the delivery of critical services are established.	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 5** CP-2, CP-8, PE-9, PE-11, PM-8, RA-9, SA-20, SR-2
		ID.BE-5: Resilience requirements to support the delivery of critical services are established for all operating states (e.g., under duress/attack, during recovery, normal operations).	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 5** CP-2, CP-11, RA-9, SA-8, SA-20
	Governance (ID.GV)	**ID.GV-1:** An organizational cybersecurity policy is established and communicated.	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 5** -1 controls from all security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners.	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev. 5** PS-7, **PS-9,** PM-1, PM-2, PM-29
		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed.	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 5** -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks.	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 5** PM-3, PM-7, PM-9, PM-10, PM-11, PM-28, RA-1, RA-2, RA-3, SA-2
	Risk Assessment (ID.RA)	**ID.RA-1:** Asset vulnerabilities are identified and documented.	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 5** CA-2, CA-5, CA-7, CA-8, PM-4, PM-15, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources.	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 5** PM-15, PM-16, RA-10, SI-5
		ID.RA-3: Internal and external threats are identified and documented.	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 5** PM-12, PM-16. RA-3, RA-10, SI-5
		ID.RA-4: Potential business impacts and likelihoods are identified.	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev.** 5 CP-2, PM-9, PM-11, RA-2, RA-3, RA-9
		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-16,PM-28, RA-2, RA-3,
		ID.RA-6: Risk responses are identified and prioritized.	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev.** 5 CA-5, PM-4, PM-9, PM-28, RA-7
	Risk Management Strategy (ID.RM)	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders.	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 5** PM-9, PM-28
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed.	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev.** 5 PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector-specific risk analysis.	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 5** PM-8, PM-9, PM-11, RA-9
	Supply Chain Risk Management (ID.SC)	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders.	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 5 PM-30,** SA-9, SR-1, SR-2, SR-3, SR-5
		ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process.	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8,

Function	Category	Subcategory	Informative References
			4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev.** 5 PM-9, RA-3, SA-15, SR-2, SR-3, SR-5, SR-6
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures that are designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev.** 5 SA-4, SA-9, SR-2, SR-3, SR-5
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluation to confirm that they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev.** 5 AU-6, CA-2, CA-7, PS-7, SA-9, SA-11
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers.	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 5** CP-2, CP-4, IR-3, IR-4, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC)**	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes.	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 5** AIA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11, IA-12
		PR.AC-2: Physical access to assets is managed and protected.	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5,

Function	Category	Subcategory	Informative References
			A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 5 PE-1,** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9
		PR.AC-3: Remote access is managed.	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 5** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed and incorporate the principles of least privilege and separation of duties.	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev.** 5 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 5** AC-4, AC-10, SC-7, SC-10, SC-20
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions.	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 5** AC-16, IA-1, IA-2, IA-4, IA-5, IA-8, IA-12, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals' security and privacy risks and other organizational risks).	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 5** AC-14, IA-1, IA-2, IA-3, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT)	**PR.AT-1:** All users are informed and trained.	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev.** 5 AT-2, PM-13, PM-14
		PR.AT-2: Privileged users understand their roles and responsibilities.	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev.** 5 AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities.	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev.** 5 AT-3, PS-7, SA-9
		PR.AT-4: Senior executives understand their roles and responsibilities.	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev.** 5 AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities.	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 5** AT-3, CP-3, IR-2, PM-13
	Data Security (PR.DS)	**PR.DS-1:** Data at rest is protected.	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev.** 5 MP-2, MP-3, MP-4, MP-5, MP-6, MP-7, MP-8, SC-28
		PR.DS-2: Data in transit is protected.	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 5** SC-8, SC-11
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition.	· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 5** CM-8, MP-6, PE-16, PE-20
		PR.DS-4: Adequate capacity to ensure availability is maintained.	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 5** AU-4, CP-2, PE-11, SC-5
		PR.DS-5: Protections against data leaks are implemented.	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 5** AC-4, AC-5, AC-6, AU-13, PE-19, PS-6, SC-7, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity.	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 5** SSI-7, SI-10

Function	Category	Subcategory	Informative References
		PR.DS-7: The development and testing environments are separate from the production environment.	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 5** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity.	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 5** SA-10
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained to incorporate security principles (e.g., concept of least functionality).	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 5** CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A system development life cycle to manage systems is implemented.	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 5** SA-3, SA-4, SA-8, SA-10, SA-11
		PR.IP-3: Configuration change control processes are in place.	· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 5** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested.	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev.** 5 CP-4, CP-6, CP-9

Function	Category	Subcategory	Informative References
		PR.IP-5: Policies and regulations regarding the physical operating environment for organizational assets are met.	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev.** 5 PE-1
		PR.IP-6: Data is destroyed according to policy.	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev.** 5 MP-6, SR-12
		PR.IP-7: Protection processes are improved.	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 5** CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6
		PR.IP-8: The effectiveness of protection technologies is shared.	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 5** AC-21, CA-7, CP-2, IR-8, SI-4
		PR.IP-9: Response plans (i.e., incident response and business continuity) and recovery plans (i.e., incident recovery and disaster recovery) are in place and managed.	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-7, CP-10, IR-1, IR-7, IR-8, IR-9
		PR.IP-10: Response and recovery plans are tested.	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev.** 5 CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening).	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev.** 5 PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21
		PR.IP-12: A vulnerability management plan is developed and implemented.	· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02 · **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 5** RA-1, RA-3, RA-5, SI-2
	Maintenance (PR.MA)	**PR.MA-1:** The maintenance and repair of organizational assets are performed and logged with approved and controlled tools.	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev.** 5 MA-1, MA-2, MA-3, MA-5, MA-6
		PR.MA-2: The remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access.	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 5** MA-4
	Protective Technology (PR.PT)	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy.	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 5** AAU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU-16
		PR.PT-2: Removable media is protected and its use restricted according to policy.	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 5** MP-1, MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
			· **CIS CSC** 3, 11, 14

Function	Category	Subcategory	Informative References
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	· **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 5** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected.	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 5** AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47
		PR.PT-5: Mechanisms (e.g., fail-safe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations.	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 5** CP-7, CP-8, CP-11, CP-13, PE-11, PL-8, SC-6
DETECT (DE)	**Anomalies and Events (DE.AE)**	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed.	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 5** AC-4, CA-3, CM-2, SC-16, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods.	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, RA-5, SI-4
		DE.AE-3: Event data are collected and correlated from multiple sources and sensors.	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: The impacts of events are determined.	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established.	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 5** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM)	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16 · **COBIT 5** DSS01.03, DSS03.05, DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events.	· **COBIT 5** DSS01.04, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 · **NIST SP 800-53 Rev. 5** CA-7, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events.	· **CIS CSC** 5, 7, 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 · **NIST SP 800-53 Rev. 5** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected.	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev. 5** SC-44, SI-3, SI-4, SI-8
		DE.CM-5: Unauthorized mobile code is detected.	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 5** SC-18, SC-44, SI-4
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events.	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 5** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 5** AU-12, CA-7, CM-3, CM-8, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed.	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 5** RA-5
	Detection Processes (DE.DP)	**DE.DP-1:** The roles and responsibilities for detection are well-defined to ensure accountability.	· **CIS CSC** 19 · **COBIT 5** APO01.02**,** DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 5** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements.	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 5** CA-1, CA-2, CA-7, PM-14, SI-1, SI-4, SR-1, SR-9, SR-10, all –1 controls
		DE.DP-3: Detection processes are tested.	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 5** CA-2, CA-7, SI-3, SI-4, PM-14

Function	Category	Subcategory	Informative References
		DE.DP-4: Event detection information is communicated.	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 5** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved.	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 5**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP)**	**RS.RP-1:** A response plan is executed during or after an incident.	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 5** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO)	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed.	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 5** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria.	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 5** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans.	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans.	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8, PE-6
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness.	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 5** PM-15, SI-5
	Analysis (RS.AN)	**RS.AN-1:** Notifications from detection systems are investigated.	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 5** AU-6, CA-7, IR-4, IR-5, PE-6, RA-5, SI-4
		RS.AN-2: The impact of an incident is understood.	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, RA-3
		RS.AN-3: Forensics are performed.	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 5** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans.	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-5, IR-8, RA-3
		RS.AN-5: Processes are established to receive, analyze, and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g., internal testing, security bulletins, or security researchers).	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 5** CA-1, CA-2, RA-1, PM-4, PM-15, RA-7, SI-5, SR-6
	Mitigation (RS.MI)	**RS.MI-1:** Incidents are contained.	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 5** IR-4
		RS.MI-2: Incidents are mitigated.	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 5** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks.	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 5** CA-2, CA-7, RA-3, RA-5, RA-7
	Improvements (RS.IM)	**RS.IM-1:** Response plans incorporate lessons learned.	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated.	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP)**	**RC.RP-1:** A recovery plan is executed during or after a cybersecurity incident.	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 5** CP-10, IR-4, IR-8
	Improvements (RC.IM)	**RC.IM-1:** Recovery plans incorporate lessons learned.	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated.	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 5** CP-2, IR-4, IR-8
	Communications (RC.CO)	**RC.CO-1:** Public relations are managed.	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4 · **NIST SP 800-53 Rev. 5** IR-4

Function	Category	Subcategory	Informative References
		RC.CO-2: Reputation is repaired after an incident.	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 5** IR-4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders and executive and management teams.	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 5** CP-2, IR-4