Draft NISTIR 8310

Cybersecurity Framework Election Infrastructure Profile

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

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8310-draft

NIST
National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NISTIR 8310

Cybersecurity Framework Election Infrastructure Profile

Mary Brady*
Software and Systems Division
Information Technology Laboratory

Gema Howell
Applied Cybersecurity Division
Information Technology Laboratory

Christina Sames
Marc Schneider
Julie Snyder
David Weitzel
The MITRE Corporation
McLean, VA

Joshua M. Franklin**
The Turnout, LLC
Silver Spring, MD

**Former employee; all work for this publication was done while at NIST*
***Former employee; all work for this publication was done while at The Turnout, LLC*

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8310-draft

March 2021

U.S. Department of Commerce
Gina Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8310
82 pages (March 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8310-draft

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *March 29, 2021* through *May 14, 2021*

National Institute of Standards and Technology
Attn: Applied Cybersecurity Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 2000) Gaithersburg, MD 20899-2000
Email: NISTIR-8310-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

This document is a Cybersecurity Framework (CSF) Profile developed for voting equipment and information systems supporting elections. This Election Infrastructure Profile can be utilized by election administrators and IT professionals managing 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. The Profile is meant to supplement but not replace current cybersecurity standards and industry guidelines that the election administrators are already leveraging.

Keywords

Cybersecurity Framework (CSF); 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 those involved 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)

Maurice Turner
Center for Democracy and Technology (CDT)

Benjamin Long
NIST

Michael South
Amazon

The authors also wish to thank the participants of the August 27-28, 2019 workshop to develop a Cybersecurity Framework (CSF) 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.

Note to Reviewers

We look forward to reviewing all of your comments. We'd also appreciate your feedback on the following questions:

- Does this profile meet your needs?
- Are there specific sections more/less helpful?
- Are there additional election security resources that would be helpful to include?
- Share any thoughts about the separation of of Mission Objective 1 into 1a and 1b (see Section 5).

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

[2] For Election Infrastructure charters and membership details, refer to the following Department of Homeland Security weblink: https://www.dhs.gov/government-facilities-election-infrastructure-charters-and-membership, last published 8 May 2019, and accessed on 25 September 2019.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or
b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:
    i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or
    ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: NISTIR-8310-comments@nist.gov, with the Subject: “NISTIR 8310 Call for Patent Claims”

Table of Contents

List of Appendices

List of Figures

List of Tables

1 Introduction

The NIST Cybersecurity Framework (CSF) is a voluntary risk-based assemblage of industry standards and best practices designed to help organizations manage cybersecurity risks [1]. The Framework, created through collaboration between government and the private sector, uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without imposing additional regulatory requirements. Although the CSF presents a variety of mitigations, many sectors and industries have opted to create their own prioritization of the CSF, known as a "CSF profile". Elections are no different, as government officials charged with the conduct of elections have their own metrics for success, priorities, and threat profile. Election infrastructure may come under cyber attack or be subject to natural disasters, and the appropriate defenses and contingencies should be identified and tailored to the subsector's needs.

1.1 Purpose

This profile was developed to take a broad look at the entire election infrastructure and to engage with election stakeholders to understand their mission objectives and priorities. 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, including the following:

- To highlight high priority security expectations,
- To perform a self assessment comparison of current risk management practices, or
- As a baseline profile or example profile to reference when developing one's own.

1.2 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, 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 or safety, or any combination thereof [2]. This Profile covers election infrastructure systems that include voting equipment and information systems that support elections and is further defined in Section 2. This CSF Profile is not intended to cover every aspect of information technology (IT) used within elections, nor cover 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.

1.3 Audience

The intended audience of this specification includes election officials, manufacturers and developers of voting systems, as well as others in the election community including the general public. Election processes are deceptively complex, thus some background in election administration or technology is useful in understanding the material in this specification. Knowledge of cybersecurity concepts is also helpful.

1.4 Document Structure

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

- Section 2 provides an overview of election infrastructure, discussing the types of information systems used for elections and supporting voting activities.
- Section 3 discusses the main elements of the CSF, what defines a CSF profile, and how it all relates to this Election Infrastructure Profile.
- Section 4 describes the methodology used to develop the Elections Infrastructure CSF Profile.
- Section 5 presents the mission objectives, which represent the granular outcomes that support the mission of the Election Infrastructure subsector.
- Section 6 summarizes the subcategories selected for the CSF profile.
- Section 7 details specific prioritization for CSF subcategories for the Elections Infrastructure sub-sector.

The document also contains the following supporting material:

- References – a list of references used in the development of this document
- Appendix A: Acronyms – selected acronyms and abbreviations used in this publication
- Appendix B: Workshop Antendees – a list of the attendees who registered to attend the election profile workshop
- Appendix C: Informative References – Cybersecurity Framework informative references

2 Overview of Election Infrastructure

As previously stated, the Elections Infrastructure subsector was created in 2017 under the Government Facilities Sector[2]. The following graphic, created by CISA, identifies the components of the election process that are included in the election infrastructure.

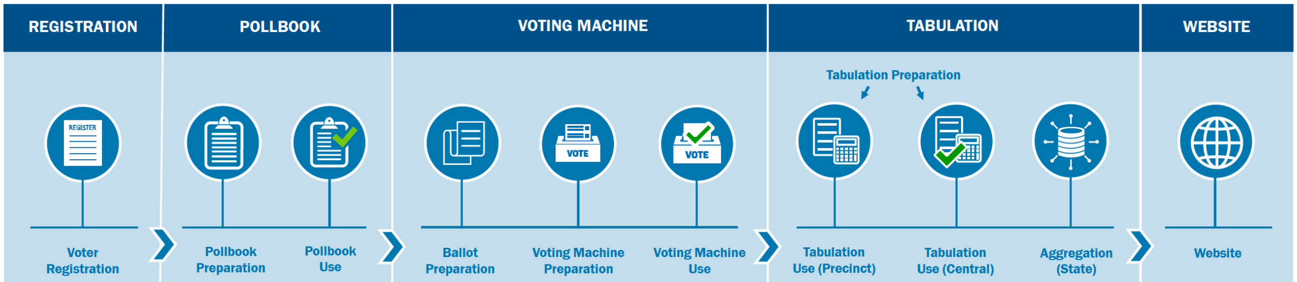

Figure 1 – CISA Election Infrastructure and Processes Infographic [3]

2.1 Exploring the Elections 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. Building on the CISA definition of election infrastructure, the following types of systems fall within the definition of Election Infrastructure[4]:

- *Voter registration databases*: Databases storing the list of citizens eligible to vote and often personally identifiable information (PII) that can be used to determine where a voter votes. This PII may also be used to authenticate them to a poll worker. Voter registration databases may have an internet-facing web application allowing voters to register and validate their information online.
- *Voting machines*: Also known as voting systems, these embedded devices enable voters to cast their ballots. These may be touchscreen, optical scan, or some type of hybrid voting system. These devices 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 (such as the counting, auditing and displaying of election results, and post-election reporting to certify and validate result*s): This 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.
- *Storage facilities for election and voting system infrastructure*: Commonly government facilities, but may also include schools, churches, etc.
- *Polling places, to include early voting locations, and other voting infrastructure*: The physical locations where US citizens cast their vote, including vote centers and ballot drop boxes.

This profile follows CISA's definition of the Election Infrastructure and excludes political action committees, campaigns, and any other non-state or local government election-related groups.

2.2 Relationship to the Voluntary Voting System Guidelines (VVSG)

The VVSG is a collection of requirements allowing voting systems to be tested against the federal government's voting system testing and certification process[5]. The types of requirements within the VVSG range from general election functionality, such as supporting various types of ballot logic and supporting multiple languages, to also including cybersecurity and human factors needs. The 2002 Help America Vote Act (HAVA)[6] mandates that the U.S. Election Assistance Commission (EAC) set and maintain the requirements. The VVSG contains granular requirements that specific implementations of voting systems can be tested against. The scope of the VVSG relates to the portion of the profile that covers *voting machines,* but the Election Infrastructrure profile itself covers many other systems as mentioned previously in Section 2.1. The Elections Infrastructure Profile does not supersede the VVSG, as each document fulfills a different need within government and industry.

3 Overview of the CSF

The CSF assists organizations in managing and reducing cybersecurity risk as well as fostering risk and cybersecurity management communications amongst both internal and external stakeholders. The CSF consists of three main components: the Core, Implementation Tiers, and Profiles. The Core is a catalog of desired cybersecurity activities and outcomes using common language that is easy to understand. A CSF Profile is an alignment of organizational requirements, objectives, risk appetite, and resources against the desired outcomes of the Framework Core. Profiles are primarily used to identify and prioritize opportunities for improving cybersecurity at an organization. Implementation Tiers guide organizations to 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. This document focuses on the use of the Framework Core to develop an Election Infrastructure Profile.

3.1 The Framework Core

The Framework Core presents industry standards, guidelines, and practices in a manner that allows cybersecurity activities and outcomes to be clearly expressed to all levels of an organization, from the executives level to the individuals with operational job roles. The Core identifies Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

3.1.1 Core Functions

The Framework Core consists of five continuous Functions—Identify, Protect, Detect, Respond, Recover. Together, these functions provide a strategic view of an organization's cybersecurity posture. The five Functions of the Framework Core are defined below[1]:

- **Identify** – Develop the organizational understanding to manage cybersecurity risk 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 the 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.

- **Protect** – Develop and implement the appropriate safeguards to ensure 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.

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

- **Respond** – Develop and implement the appropriate activities to take action regarding a detected cybersecurity event. The activities in the Respond Function support the ability to contain the impact of a potential cybersecurity event. Examples of outcome Categories within this Function include: Response Planning; Communications; Analysis; Mitigation; and Improvements.

- **Recover** – Develop and implement the appropriate activities to maintain plans for resilience and to 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 from a cybersecurity event. Examples of outcome Categories within this Function include: Recovery Planning; Improvements; and Communications.

3.1.2 Core Categories and Subcategories

The Core identifies Categories and Subcategories for each Function, and matches them with example Informative References such as existing standards, guidelines, and practices for each Subcategory.

The Core Categories serve as the basis and context for the development of CSF Profiles and mission objectives. The 23 categories spread across those Functions described above: Identify, Protect, Detect, Respond, Recover.

Table 1 - CSF 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

Function Unique Identifier	Function	Category Unique Identifier	Category
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

There are 108 Subcategories which support achieving the Catorgies by providing specific outcomes through technical and/or management activities. A list of the Subcategories can be found in Section 7.

3.2 Applying the Cybersecurity Framework

The Elections Infrastruture Profile defines specific practices to address the Framework Core. It is the next layer of detail for implementing cybersecurity best practices for each category expressed in the Framework. It is intended to support cybersecurity decisions based on needs expressed by those charged with the conduct of elections in the US. The Profile can be characterized as the alignment of standards, guidelines, and practices to the Framework Core in a practical implementation scenario.

4 Profile Development Methodology

This section discusses the approach used to create the Elections Infrastructure Profile. A description of the workshops held to identify relevant mission objectives is also provided.

4.1 Election Profile Workshop

On August 27-28, 2019, the National Institute of Standards and Technology (NIST) conducted a workshop to gather stakeholder input to contribute to the development of a CSF Profile for election infrastructure in the United States. The workshop included participants from the Election Infrastructure Subsector [3](EIS) Government Coordinating Council (GCC) and the Sector Coordinating Council (SCC)

[7], as well as 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 with respect to achieving election security, as prioritized by the workshop participants;
- for each mission objective, identifying and ranking the top three CSF categories (out of 23 available) that participants consider most important for accomplishing that objective securely, as well as additional categories considered important for that objective

4.2 Follow-on Working Sessions Profile Development

The final step in the methodology was the development of this Election Infrastructure profile. This Profile provides the results of the workshop and follow-on working sessions with stakeholders and also of post-workshop analysis. The aggregated ranking from the initial workshop enabled post-workshop analysis to define a prioritization of categories considered moderate, moderate-to-possibly-high, and high priority (see Section 6), and were used to facilitate subsequent ranking of the most important cybersecurity subcategories (out of a total of 108) for each mission objective (see Section 7).

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

5 Election Infrastructure Mission Objectives

Ten mission objectives, listed below, and their relative priority based on stakeholder rating, emerged from 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 On-Going 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 conveying our preliminary understanding of relevant activities, with rationale for top mission objectives.

1. **Conduct and Oversee Voting Period Activities**†. This mission objective encompasses all activities directly associated with the election *during the time when voters can submit their votes.* This mission objective includes all voting period activities required to allow for the following: *remote voting (absentee/military/overseas), in-person early voting, election day voting, and provisional ballot voting*. During the working sessions it was decided to bifurcate Mission Objective #1 into two phases.

   - Phase **1A** addresses those activities associated with vote capture, such as early voting, election day voting and absentee voting, and
   - Phase **1B** addresses those activities associated with vote aggregation, tabulation, canvassing, recounting (as necessary), and enumeration through certification and reporting of election results.

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

   A list of activities relevant to this mission objective includes:
   - Open/close polls
   - Voting system setup within the polling place
   - Vote and submit ballots

- Voter check-in and eligibility determination
- Send Ballots by mail/electronically
- Election night reporting
- Vote aggregation, tabulation, canvassing, recounting (as necessary), and enumeration
- Transmit/send tabulation results to central tabulation center/back office
- Certification and publication of election results

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

2. **Prepare and Maintain Election Systems**†. This mission objective encompasses all aspects of preparing and maintaining systems used for elections (with the exception of voter registration systems and back-end services, such as email, which workshop participants deemed worthy of coverage in separate mission objectives). This mission objective involves a holistic approach to the processes and procedures for acquiring, testing and certifying, configuring, and protecting election systems. The following is a list of some activities relevant to this mission objective:
    - Procure voting system and supplies (keyboards, monitors, mice, etc.).
    - Test and certify election systems
    - Update election systems
    - Store election systems in a secure location

    Rationale: This mission objective represents essential precursor activities critical to *Conduct and Oversee Voting Period Activities*, Mission Objective 1.

3. **Process and Maintain Voter Registration**†. This mission objective encompasses all aspects of data and systems 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* including election day registration, where allowed. The following is a list of some activities relevant to this mission objective:
    - Maintain voter registration list/database
    - Maintain voter registration website
    - Process voter registrations
    - Release information to 3rd parties as allowed or required by law

    Rationale: This mission objective represents critical precursor activities vital to ensuring qualified citizens can properly vote and maintaining the integrity and security of voter information, upon which hinges the confidence of the electorate in an election outcome.

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. The following is a list of some activities relevant to this mission objective:
    - Establish voting locations (polling places or vote centers)
    - Transport and store equipment, ballots, etc., to voting locations
    - Process candidate filing 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 critical to *Conduct and Oversee Voting Period Activities* (Mission Objective 1).

5. **Perform On-Going Election Administration Functions**. This mission objective encompasses administrative functions necessary for day-to-day operations *exclusively related to elections.* The following is a list of some activities relevant to this mission objective:
    - Acquisition of election-related tools and applications
    - Staff and acquire support services/contracts
    - Data hygiene
    - Manage chain of custody
    - Monitor and comply with law & policy
    - 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 these three high-level categories: *quality audit, security audit, and tabulation audit*. The following is a list of some activities relevant to this mission objective, categorized by audit type:
    - *Security Audits*
        - Security audit of voting systems prior to election day
        - Security audit of voting systems on election day
        - System audit
        - Compliance audit
        - Chain-of-custody audit
    - *Tabulation Audits*
        - Hand-count audit
        - Risk-limiting audit
        - Ballot comparison audit
    - *Quality Audits*
        - Logic & accuracy audit

  - Ballot content audit
  - Public test (mock election) – audit prior to initial voting
  - Parallel testing – running 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 the certification and publishing of election results. This mission objective covers the tasks necessary to officially close out the election. The following is a list of some activities relevant to this mission objective:
   - Retain and secure election materials
   - Check poll voting equipment
   - Pay fee 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 (such as the Governor and Secretary of State), security/law enforcement (e.g., DHS, FBI), the press, and the public during and after events which impact, or appear to impact, the conduct of a free and fair election. The following is a list of some activities relevant to this mission objective:
   - Updating and managing social media accounts
   - Process 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 general support services necessary for day-to-day operations. These include tools and applications, such as email, support services (whether staffed/acquired internally or contracted) and IT supply chain management. The following represent a list of some activities relevant to this mission objective:
   - Support for email system
   - Support for other general services
   - Support for state systems necessary for elections (e.g., Motor Vehicle Administration (MVA) records)

10. **Maintain Workforce**. This mission objective encompasses functions associated with effectively acquiring, training and leading the personnel essential to the successful conduct of free and fair elections. Elections employ one of the largest temporary workforces in the nation. The following is a list of some activities relevant to this mission objective:
    - Provide training
    - Familiarize processes and procedures

- Recruit poll workers for a specific election
- Pay and reimburse poll workers
- Protect election/poll workers' sensitive information
- Mitigate insider threats

6 Summary Framework Category Prioritization

This section summarizes the relative importance of Cybersecurity Framework categories to achieving each mission objective. For each mission objective, stakeholders identified the top category from each of the five functions they considered most important for achieving the mission objective securely and ranked them in order of importance. The top three category selections were scored numerically to achieve a priority ranking. Beyond these top three, the stakeholders also identified the top category from the remaining functions to ensure each MO was scored with the five CSF categories (one from each function) they considered most important to achieving the mission objective. This data was used to identify the categories that were considered moderate, moderate-to-possibly-high, and high priority for 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 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 achieving the mission objective securely (≥3 votes and ≤ 2.0 average rank OR ≥ 5 votes and ≤ 2.5 average rank)
- **Moderate-Possibly-High (M-H)** - Possibly high priority due to number of votes and score (≥5 votes and ≤ 3.0 average OR ≥3 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.

Note that all categories should be addressed when relevant to an organization and mission objective, even if they do not appear in the tables below. The intent of this exercise is to designate High and Moderate Priority categories (and later, subcategories) to help organizations first focus on the cybersecurity activities that are most critical to each mission objective. Designating categories as “N/A” in the tables below does not mean they are not important, it simply means they are not considered to be the most urgent focus for that mission objective (MO). Mission Objective 1a and 1b received the same weighted scores and so the priority categories are combined into one table (Table 3).

6.1 Priority Categories by Mission Objective

Table 3 - Conduct and Oversee Voting Period Activities (MO #1a and #1b)

CSF 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

CSF Function	High Priority	Moderate-Possibly High Priority	Moderate Priority
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)

CSF 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)
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)

CSF 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)

CSF 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)	N/A

CSF Function	High Priority	Moderate-Possibly High Priority	Moderate Priority
		Information Protection Processes & Procedures (PR.IP)	
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 On-Going Election Administration Functions (MO #5)

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

CSF 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)

CSF 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)

CSF 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)

CSF 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)

CSF 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)

6.2 Summary Table

The following table provides a summary view of CSF category prioritization, derived from stakeholder scoring, to aid in comparing similarities and differences across all mission objectives. Initial observations and items under consideration include the following:

- Strong emphasis on IDENTIFY and PROTECT exists across all mission objectives.
- Strong emphasis exists on several categories across several mission objectives, in particular:
  - 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

	Mission Objectives										
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											

	Mission Objectives										
Categories	***1a***	***1b***	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***
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	
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		

7 Priority Subcategories by Mission Objective

This profile summary of priority subcategories in the charts below can be used in several ways, including the following:

- Highlighting high priority security expectations,
- Performing a self assessment comparison of current risk management practices, or
- As a baseline profile or example profile to reference when developing one's own.

This section provides an example of how an election stakeholder may prioritize their approach to addressing the Subcategories. Each State or election jurisdiction may have different priorities and when making cybersecurity decisions they may adjust the priorities to meet their unique needs.

The initial Category rankings informed the level of priority given to the sub-categories (outcomes-based activities). For each mission objective, only subcategories of those categories that had been identified as moderate, moderate-to-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 the most urgent and two dots considered less so. Each of these subcategories were ranked to determine whether it was considered to be of high (●●●), moderate (●●), or average (●) urgency for achieving the mission objective securely. To assist with addressing the subcategories, Appendix C— lists informative references 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 delivery of critical services are established	●	●	●	●	●	●●●	●	●	●	●	●●
		ID.BE-5: Resilience requirements to support 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 & 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	•	•	•	•	•	•	•	•	•	•	•

681 **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	●	●	●	●	●	●	●	●	●	●	●

682

683

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

Function	Category	Subcategory	Mission Objectives										
			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 risk. The organization has established and implemented the processes to identify, assess and	**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.	●	●	●	●	●	●	●	●	●	●●●	●
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	●	●	●	●	●	●	●	●	●	●●	●

	manage supply chain risks.	**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, or devices, and to authorized 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, incorporating 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 provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	●●	●●	●	●	●	●●	●	●	●	●●●	●●●
		PR.AT-2: Privileged users understand roles and responsibilities	●●●	●●●	●	●	●●●	●●●	●	●	●	●●●	●●●
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand roles and responsibilities	●	●●●	●	●	●●	●●	●	●	●	●●	●●
		PR.AT-4: Senior executives understand roles and responsibilities	●	●	●	●	●●	●	●	●	●	●	●
		PR.AT-5: Physical and information security personnel understand 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 environment(s) 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 protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g., concept of least functionality)	•	•	•	•	•••	•	•	••	•	•	•
		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: Policy 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	•	•	•	•	•	•	•	•	•	•	•

		PR.IP-8: Effectiveness of protection technologies is shared	●	●	●	●	●●	●	●	●	●●●	●	●
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (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):** Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets is performed and logged in a timely manner, with approved and controlled tools	●	●	●	●	●	●	●	●	●	●	●
		PR.MA-2: 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 principles 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., failsafe, 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 impact of events is 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: Impact of events is 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):** The information system 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	●	●	●	●●●	●	●	●	●	●	●●●	●

707 **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	●	●	●●	●	●	●	●	●	●	●	●

708

709

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:** 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 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	●	●	●	●	●	●	●	●	●●	●	●

716 **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 response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	●	●	●	●	●	●	●	●	●	●	●
		RS.AN-2: The impact of the 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)	●	●	●	●	●	●	●	●	●	●	●

717

718

719 **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 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	●	●	●●●	●	●	●	●	●	●	●	●

720

721

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	●	●	●	●	●	●	●	●	●	●	●

725 **Table 34 - Recovery Planning (RC.RP) Subcategories**

Function	Category	Subcategory	Mission Objectives										
			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 timely restoration of systems or assets affected by cybersecurity events.	**RC.RP-1:** Recovery plan is executed during or after cybersecurity incident	●●●	●●●	●●	●●●	●●●	●●●	●●●	●●●	●	●●●	●●●

726

727

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 (2020) *Election Infrastructure Cyber Risk Assessment. Critical Infrastructure Security and Resilience Note*, July 28, 2020; 1400 EDT. Available at https://www.cisa.gov/sites/default/files/publications/cisa-election-infrastructure-cyber-risk-assessment_508.pdf

[4] U.S. Department of Homeland Security (2020) *Election Security*. Available at https://www.dhs.gov/topic/election-security

[5] U.S. Election Assistance Commission (2020) 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 (2020) 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
CSF	Cybersecurity Framework
DE	Detect
DHS	Department of Homeland Security
DP	Detection Processes
DS	Data Security
EI	Election Infrastructure
EIS	Election Infrastructure Subsector
FBI	Federal Bureau of Investigation
GCC	Government Coordinating Council
GV	Governance
ID	Identity
IM	Improvements
IP	Information Protection Processes and Procedures
IT	Information Technology
MA	Maintenance
MI	Mitigation
MO	Mission Objective
MVA	Motor Vehicle Administration
NIST	National Institute of Standards and Technology
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 attendees that registered to attend the Election Infrastructure Profile Workshop that was held on August 27th and 28th, 2019.

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	MITRE
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	MITRE
17	Macias	Ryan Stephen	Lafayette Group – on behalf of CISA
18	Martin-Rozumitowicz	Beata	IFES

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

Appendix C—Informative References

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

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. 4** 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. 4** CM-8, PM-5
		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. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, 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 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, 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. 4** CP-2, PS-7, PM-11
	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. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** 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. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for 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. 4** CP-8, PE-9, PE-11, PM-8, SA-14

Function	Category	Subcategory	Informative References
		ID.BE-5: Resilience requirements to support 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. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV)	**ID.GV-1:** 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. 4** -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 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
		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. 4** -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. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment	**ID.RA-1:** Asset vulnerabilities are identified and	· **CIS CSC** 4

Function	Category	Subcategory	Informative References
	(ID.RA)	documented	· **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. 4** CA-2, CA-7, CA-8, 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. 4** SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, 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. 4** RA-3, SI-5, PM-12, PM-16
		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 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
		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. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
	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. 4** PM-9
		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. 4** 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. 4** SA-14, PM-8, PM-9, PM-11
	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. 4** SA-9, SA-12, PM-9
		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, 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

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		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.	· **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. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm 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. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		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. 4** CP-2, CP-4, IR-3, IR-4, IR-6, 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. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11

Function	Category	Subcategory	Informative References
		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, 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. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		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. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating 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. 4** 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. 4** AC-4, AC-10, SC-7

Function	Category	Subcategory	Informative References
		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. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, 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 · **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. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, 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. 4** AT-2, PM-13
		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. 4** AT-3, PM-13

Function	Category	Subcategory	Informative References
		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. 4** PS-7, SA-9, SA-16
		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. 4** 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. 4** AT-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 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, 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. 4** SC-8, SC-11, SC-12

Function	Category	Subcategory	Informative References
		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. 4** CM-8, MP-6, PE-16
		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. 4** AU-4, CP-2, 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. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, 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. 4** SC-16, SI-7
		PR.DS-7: The development and testing environment(s) are separate from the production	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04

Function	Category	Subcategory	Informative References
		environment	· **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** 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. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP)	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	· **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. 4** 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. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		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. 4** CM-3, CM-4, SA-10

Function	Category	Subcategory	Informative References
		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. 4** CP-4, CP-6, CP-9
		PR.IP-5: Policy 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. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		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. 4** MP-6
		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. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: 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. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and	· **CIS CSC** 19

Function	Category	Subcategory	Informative References
		Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **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. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		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. 4** 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 · **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. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, 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. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA)	**PR.MA-1:** 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. 4** MA-2, MA-3, MA-5, MA-6

Function	Category	Subcategory	Informative References
		PR.MA-2: 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. 4** 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. 4** AU Family
		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. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities	· **CIS CSC** 3, 11, 14 · **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,

Function	Category	Subcategory	Informative References
			SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** 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. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, 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. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, 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. 4** AC-4, CA-3, CM-2, 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. 4** AU-6, CA-7, IR-4, 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. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** 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. 4** 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. 4** AC-2, 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. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect	· **CIS CSC** 5, 7, 14, 16

Function	Category	Subcategory	Informative References
		potential cybersecurity events	· **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. 4** 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 · **NIST SP 800-53 Rev. 4** SI-3, 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. 4** SC-18, SI-4, SC-44
		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. 4** 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. 4** AU-12, CA-7, CM-3, CM-8, PE-3, 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

Function	Category	Subcategory	Informative References
			· **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP)	**DE.DP-1:** 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. 4** 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. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		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. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		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. 4** 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

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP)**	**RS.RP-1:** 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. 4** 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. 4** 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. 4** 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. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		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 · **ISO/IEC 27001:2013** Clause 7.4

Function	Category	Subcategory	Informative References
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		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. 4** SI-5, PM-15
	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. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the 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. 4** CP-2, IR-4
		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. 4** 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. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive,	· **CIS CSC** 4, 19

Function	Category	Subcategory	Informative References
		analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	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 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** 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. 4** 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. 4** CA-7, RA-3, RA-5
	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. 4** 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. 4** CP-2, IR-4, IR-8
RECOVER	**Recovery**	**RC.RP-1:** Recovery plan is executed during or after	· **CIS CSC** 10

Function	Category	Subcategory	Informative References
(RC)	Planning (RC.RP)	a cybersecurity incident	· **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** 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. 4** 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. 4** 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
		RC.CO-2: Reputation is repaired after an incident	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4
		RC.CO-3: Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4