Cross-Sector Cybersecurity Performance Goals

Version 2.0

December 2025

Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see [Traffic Light Protocol (TLP) Definitions and Usage](#).

CONTENT

BACKGROUND AND CONTEXT

OUR CHALLENGE AHEAD

CISA works every day with government, private sector, and international partners to gain unique insight into the state of cybersecurity across U.S. critical infrastructure and the nature of the threat landscape. Through these partnerships[1] and our own cyber assessments, threat hunting, and incident response efforts, CISA regularly observes a lack of cybersecurity best practices in critical infrastructure. Subject matter experts and critical infrastructure operators providing input during this document's development shared similar observations.

Each organization faces unique cybersecurity challenges. Small- and medium-sized organizations may have limited budgets, staffing, and expertise. Meanwhile, organizations with mature cybersecurity programs strive to move beyond foundational defenses to stay ahead of advanced adversaries, especially in environments that include operational technology (OT).

Cybersecurity guidance is widely available, but many organizations frequently tell us they need help with:

1. Identifying which practices yield the greatest risk reduction,
2. Prioritizing these practices for maximum impact, and
3. Communicating practice value to their senior leadership and governing bodies.

CISA developed the Cross-Sector Cybersecurity Performance Goals (CPGs) to address these needs.

The CPGs are streamlined and outcome-driven cybersecurity protections for information technology (IT) and OT environments. The CPGs provide:

- Clear, foundational practices aligned with real-world threats.
- Straightforward, outcome-oriented language to aid implementation.
- A baseline for guiding investment, benchmarking progress, and reducing risk in measurable ways.

Building on our commitment to continuous improvement and alignment with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0, we have enhanced the CPGs by adding a governance function. This new component highlights the critical role of organizational leadership in overseeing cybersecurity. It emphasizes accountability, risk management, and strategic integration of cybersecurity into day-to-day operations, reinforcing the principle that effective governance is the cornerstone of a resilient cyber posture.

We designed the CPGs to be approachable and practical. They aim to address common and impactful cyber risks with clarity and simplicity, making the CPGs accessible not only to cybersecurity practitioners but also to non-technical stakeholders, including senior executives and board members.

Numerous federal, state, local, territorial, tribal, and private sector organizations have implemented the CPGs since their initial 2022 release. Early adopters used them to benchmark baseline cybersecurity hygiene and inform cybersecurity resourcing requests. However, there has been a gap in CPG adoption between larger utilities and agencies and smaller organizations, which often struggle to translate high-level goals into concrete action. Our concern with this gap is more than hypothetical. Our nation has seen its real-world impact, from ransomware attacks that affect schools and hospitals to sophisticated nation-state campaigns that target government agencies and critical infrastructure. Collectively, these intrusions place our national security, economic security, and the health and safety of the American people at risk.

While progress has been made since the 2022 publication of the CPGs, our nation's cybersecurity risk remains abundant. CISA is releasing this CPG update to incorporate lessons learned, to align with the most recent NIST CSF revisions, and to address the following challenges:

[1] Specific partners include organizations across the 16 critical infrastructure sectors and their respective sector risk management agencies.

1. **OT cybersecurity often remains overlooked and under-resourced**. The cybersecurity industry continues to focus primarily on business IT systems, frequently neglecting the unique and significant risks posed by OT environments. Manufacturers have historically designed these systems for reliability and availability, not security. They also often lack built-in protection. As more OT devices gain network connectivity, inadequate cybersecurity protections expose critical infrastructure to serious threat. Many organizations still lack dedicated OT cybersecurity programs; this is especially prevalent in organizations that view cybersecurity solely as an IT issue. OT cybersecurity programs that currently exist often fall short on basic cybersecurity practices and actionable OT-specific protections.

2. **Many organizations have not adopted fundamental security protections**. The absence of basic protections such as multifactor authentication (MFA), strong password management, and routine backups, among other foundational measures, expose critical infrastructure to damaging cyber intrusions.

3. **Small- and medium-sized organizations are left behind**. Organizations with limited resources or less mature cybersecurity programs often face challenges determining how to begin implementing reasonable cybersecurity measures. Despite existing resources, like the NIST CSF, small organizations face difficulties in identifying where to invest to try to get the greatest impact to their cybersecurity posture and how to effectively implement cybersecurity protections.[2]

4. **Lack of consistent standards and cyber maturity**. There is significant inconsistency in cybersecurity capabilities, investment, and baseline practices across critical infrastructure sectors. This inconsistency can lead to gaps that threat actors can exploit to cause functional and cascading impacts.

[2] To lower the barrier to entry, in 2023, CISA started providing Sector-Specific Goals (SSGs). These are additional voluntary practices with high-impact security measures tailored for specific critical infrastructure sectors. The SSGs build on the CPGs by addressing unique sector requirements and providing actionable measures that organizations, including small- and medium-sized businesses, can take to protect against malicious cyber activity.

CONFRONTING THE CHALLENGE

Under its statutory authority (6 U.S.C. §652), CISA provides technical assistance in the form of cybersecurity assessments and collaborates with the National Institute of Standards and Technology (NIST) and other federal partners to maintain baseline cybersecurity goals for critical infrastructure. In addition to the Cross-Sector Cybersecurity Performance Goals (CPGs), CISA works with federal sector risk management agencies (SRMAs) and the critical infrastructure community to develop additional Sector-Specific Goals (SSGs).

WHAT ARE THE CPGs?

Simply put, the CPGs are a prioritized subset of IT and OT cybersecurity practices aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. These goals are applicable across all critical infrastructure sectors. The most common and impactful threats and adversary tactics, techniques, and procedures (TTPs) observed by CISA and its government and industry partners inform the CPGs, which make them a common set of protections that all critical infrastructure entities—from large to small—should implement.

The CPGs do not reflect an all-encompassing cybersecurity program; rather, they are a minimum set of practices that organizations should implement. They aim to help critical infrastructure entities, particularly small and medium organizations, get started on their path toward a strong cybersecurity posture. As such, CISA intends for the CPGs to be a floor—not a ceiling—of cybersecurity protections organizations should implement to reduce their cyber risk. Importantly, the CPGs are **not**:

KEY CHARACTERISTICS OF THE CPGs

- A prioritized subset of cybersecurity practices
- For IT and OT
- Prioritized for risk reduction
- Informed by threats observed by CISA and its government and industry partners
- Applicable across all critical infrastructure sectors
- Intended to meaningfully reduce risk to both critical infrastructure operations and the American people

- **Comprehensive:** The CPGs do not identify all the cybersecurity practices needed to protect every organization or fully safeguard national and economic security and public health and safety against all potential risks. They represent a minimum baseline of cybersecurity practices with known risk-reduction value broadly applicable across all sectors. However, CISA is rolling out sector-specific goals that dive deeper into the unique constraints, threats, and maturity of each sector.
- **A risk management or full cybersecurity program:** The CPGs do not cover broader approaches to risk management or risk prioritization that other frameworks, such as the NIST CSF, articulate.
- **Mandated by CISA:** CISA intends for organizations to voluntarily adopt the CPGs to enable prioritization of security investments toward the most critical outcomes, in conjunction with broader frameworks, like the NIST CSF.
- **A maturity model:** The practices in the CPGs apply to all critical infrastructure organizations and are not tiered into “maturity” categories. However, the CPG Worksheet includes criteria such as “Impact,” “Cost,” and “Complexity” to help organizations internally prioritize their investment.

CISA will regularly update the CPGs according to a targeted revision cycle of 24 to 36 months.

CPG SELECTION CRITERIA

The CPGs are a subset of cybersecurity practices—selected through a process of industry, government, and expert consultation—using several criteria:

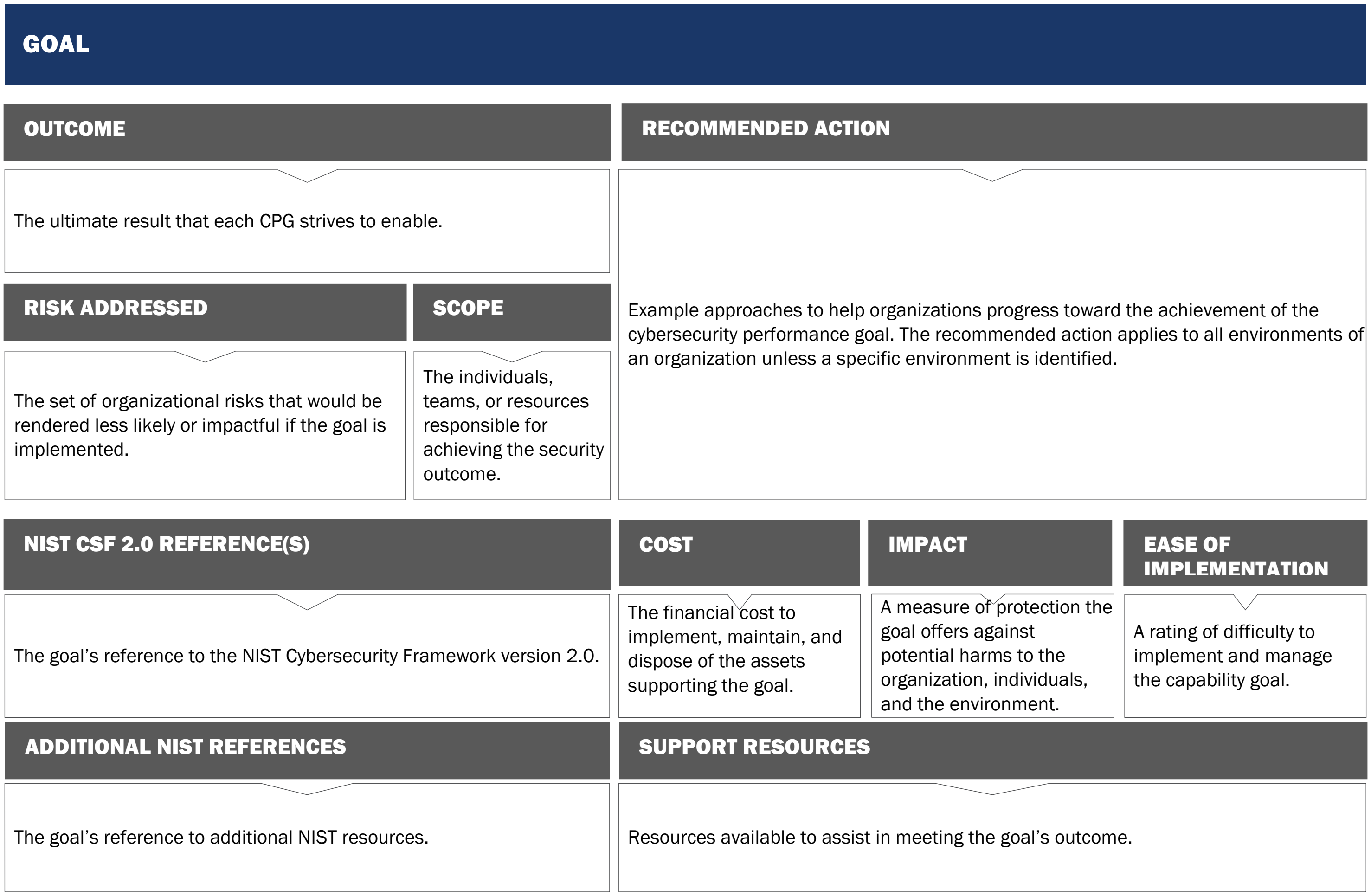
1. Demonstrated value in reducing the risk or impact of commonly observed, cross-sector threats and cyber threat actor TTPs.
2. Clear, actionable, and easily definable.
3. Reasonably straightforward and not cost-prohibitive for small- and medium-sized entities to successfully implement.

An example of a CPG that meets this criteria is: “ensuring that none of an organization’s internet-facing systems have any known exploited vulnerabilities (KEVs).” This CPG is definable, achievable, and directly reduces the risk from a known threat—that nation-state threat actors actively exploit those weaknesses in the wild. Conversely, a practice such as “implement zero trust” would not be a suitable CPG at this time. While zero trust is a very effective approach, many small organizations, who represent the CPG’s target audience, may have challenges implementing zero trust if they have not yet implemented the full set of CPGs.

CPG MODEL

This document displays the CPGs in a visual model to help readers understand not only the goals themselves, but also the intended outcomes, the risks or TTPs that the goals address—i.e., what “good” looks like—and other important information.

Each goal comprises the following components:



GOAL

OUTCOME

The ultimate result that each CPG strives to enable.

RECOMMENDED ACTION

Example approaches to help organizations progress toward the achievement of the cybersecurity performance goal. The recommended action applies to all environments of an organization unless a specific environment is identified.

RISK ADDRESSED

The set of organizational risks that would be rendered less likely or impactful if the goal is implemented.

SCOPE

The individuals, teams, or resources responsible for achieving the security outcome.

NIST CSF 2.0 REFERENCE(S)

The goal’s reference to the NIST Cybersecurity Framework version 2.0.

COST

The financial cost to implement, maintain, and dispose of the assets supporting the goal.

IMPACT

A measure of protection the goal offers against potential harms to the organization, individuals, and the environment.

EASE OF IMPLEMENTATION

A rating of difficulty to implement and manage the capability goal.

ADDITIONAL NIST REFERENCES

The goal’s reference to additional NIST resources.

SUPPORT RESOURCES

Resources available to assist in meeting the goal’s outcome.

HOW ARE THESE DIFFERENT FROM NIST CSF AND OTHER STANDARDS?

There are other existing cybersecurity guidance documents and frameworks—especially from the U.S. government. For example, the NIST CSF continues to be one of the most widely adopted and well-known cybersecurity frameworks. CISA and the broader U.S. government support all organizations adopting the NIST CSF to enable development and maintenance of a sustainable, risk-informed cybersecurity program. Based on stakeholder feedback, organizations can use the CPGs as part of a broader cybersecurity program based on the NIST CSF or other frameworks and standards.

1. **A Quick-Start Guide.** The CPGs can help organizations that may lack the cybersecurity experience, resources, or structure in place to quickly identify and implement basic cybersecurity practices. After or in parallel to applying the CPGs, organizations can continue to leverage the NIST CSF to build a holistic risk management program and implement additional NIST controls.

2. **Prioritization and Obtaining Funding.** The CPGs contain a worksheet, described below, that can help organizations with smaller or less mature cybersecurity programs prioritize which protections to implement, and communicate the importance and relative impact and cost of those protections to (non-technical) executives.

3. **NIST CSF Mappings.** Every security practice in the CPGs aligns and maps to a corresponding subcategory in the NIST CSF. Note the CPGs do not fully address each NIST CSF subcategory. For each security practice, identification of the CSF subcategory indicates a relationship between the CPG and the NIST CSF. Organizations that have already adopted and implemented the NIST CSF will not need to perform additional work to implement the relevant CPGs.

HOW TO USE THE CPGs

CPG Reference Products

There are two documents provided on the CPGs:

1. The CPG List (this document)
2. The CPG Checklist

The CPG Worksheet

In addition to the list of CPGs, there is a user-friendly worksheet for asset owners and operators to (1) review and prioritize which CPGs to implement, (2) track the current and future state of CPG implementation, and (3) clearly communicate the priorities, trade-offs, and statuses of the CPGs to other stakeholders, such as non-technical executives. This worksheet is available at CISA.gov, as well as within the CPG Assessment module of CISA's Cyber Security Evaluation Tool (CSET).

The worksheet includes general estimates of the cost, complexity, and impact of implementing each goal. Organizations can use these estimates as an aid to help inform investment strategy to address known gaps in baseline cybersecurity capability.

Using the CPG Worksheet

1. **Perform an initial self-evaluation.** Organizations should review their existing security programs and security controls to determine which CPGs they already have implemented. Organizations may have already implemented some or many of the CPGs through their adherence to existing guidance or framework, such as NIST CSF or ISA/IEC 62443, and all CPGs map to corresponding controls in those common frameworks.
2. **Identify and prioritize gaps.** Organizations should review gaps in their CPG implementation and prioritize those areas for investment based on factors such as cost, complexity, and impact, which are all included in the CPG Worksheet.
3. **Invest and execute.** Organizations can start implementing the prioritized gaps identified in Step 2. Some organizations may find materials such as the worksheet helpful when working with their leadership to request funding for cybersecurity-focused projects.
4. **Review progress regularly after 12 months.** To track progress toward improved cybersecurity practices, organizations should go through the worksheet after 12 months to capture progress, both for their own leadership as well for third parties.

CHANGES TO THE CPGs

October 2025 UPDATE: CPG 2.0

CISA has refreshed the CPGs to align with the NIST Cybersecurity Framework 2.0, incorporate three years of operational feedback, and address emerging threats with data-driven recommendations. Below is a high-level summary of what changed and why.

1. **Structural Changes – New "GOVERN" Function**
   - What changed:
     - Regrouped and renumbered existing goals to accommodate a sixth CSF function, GOVERN.
     - All previous goals were mapped into one of five functions, namely IDENTIFY, PROTECT, DETECT, RESPOND, and RECOVER.
   - Why: The new GOVERN function integrates leadership accountability, oversight, and risk management into everyday cybersecurity practices, mirroring NIST CSF 2.0's new emphasis on organizational governance.

2. **Goal Consolidations – Streamlining & Cross-Sector Alignment**
   - What changed:
     - Folded CPG 1.0.1 OT-only goals (1.B/1.C/1.D; 2.I/2.J; 2.W/2.X) into universal goals (now 1.A; 3.J; 3.S).
     - Related objectives have been merged for brevity 1.G + 1.H into 1.D and 2.T + 2.U into 3.Q.
   - Why:
     - This removes duplicate guidance, so practitioners don't need to read across multiple goals for the same control.
     - We recognize that modern infrastructures blur IT, internet of things (IoT), and OT. Thus, one goal set now covers all rather than siloed sections.
     - Small- and medium-sized entities can apply one framework across their entire estate, without confusion over domain-specific goals.

3. **Net-New Goals – Addressing Emerging Threats & Gaps**
   - What changed:
     - Added four new goals:
       - 1.B – Proactive Program Management: Builds on 1.A to encourage leaders to adapt strategies and respond to evolving threats.
       - 1.E – Managed Service Provider Risk: Captures risks from third-party providers with deep system access.
       - 3.H – Least-Privilege Enforcement: Advances zero-trust principles to mitigate lateral movement.
       - 5.A – Incident Communication Procedures: Establishes clear channels with internal teams, partners, and suppliers for crisis response.
   - Why:
     - Feedback showed that v1.0.1 didn't explicitly address ongoing program evolution, third-party dependencies, or advanced access controls. The four new goals in CPG 2.0 fill those blind spots.
     - With managed service providers now mission critical, formal risk controls are vital to prevent supply chain compromise.
     - Well-defined communication procedures help ensure transparency and coordination during incidents, reducing confusion and downtime.

4. **Deletions & Intent Preservation**
   - What changed:
     - Removed the following three v1.0.1 goals:
       - 4.C – Security.txt Deployment was folded into 2.D ("Maintain Vulnerability Disclosure/Reporting Process").
       - 3.A – Detect Relevant Threats and Tactics/Techniques/Procedures was consolidated under 4.B ("Identify Adverse Events").
       - 1.I – Vendor/Supplier Cybersecurity Requirements was merged into 1.D ("Supply Chain Incident Reporting & Vulnerability Disclosure").
   - Why:
     - These standalone items saw low adoption or overlapped with broader objectives. Every original objective still lives in the updated goals, including the outcomes of the original goals.
     - Real-world usage data and practitioner feedback indicated these standalones were confusing or underutilized.

5. **Methodology & Documentation Enhancements**

- What changed:
  - Added Cost, Impact, and Ease of Implementation ratings to the CPG Report and Checklist.
  - Replaced “Complexity” from v1.0.1 with “Ease of Implementation.”
  - Added detailed definitions and the logic behind each rating.
- Why:
  - By sharing the logic behind each score, CISA improves transparency, builds trust in the framework, and reduces guesswork.
  - The inclusion of clear definitions behind each rating is intended to aid assessors in conducting CPG assessments with a greater degree of repeatable analytic consistency.

CPG Mapping Comparison: v1.0.1 vs 2.0

CPG Mapping Comparison		
CPG v1.0.1	Is Now	CPG v2.0
1.A	=	2.A
1.B	=	1.A
1.C		
1.D		
1.E	=	2.B
1.F	=	2.C
1.G	=	1.D
1.H		
1.I	=	DELETED
2.A	=	3.A
2.B	=	3.B
2.C	=	3.C
2.D	=	3.D
2.E	=	3.G
2.F	=	3.I
2.G	=	3.E
2.H	=	3.F
2.I	=	3.J
2.J		
2.K	=	3.K
2.L	=	
2.M	=	3.L
2.N	=	3.M
2.O	=	3.N
2.P	=	2.E
2.Q	=	3.P
2.R	=	3.O
2.S	=	1.C
2.T	=	3.Q
2.U		
2.V	=	3.R
2.W	=	3.S
2.X		
3.A	=	DELETED
4.A	=	5.B
4.B	=	2.D
4.C	=	DELETED
5.A	=	6.A

CPG v2.0
Added New Goals
1.B
1.E
3.H
4.A
4.B
5.A

Updates to Cost, Impact, and Ease of Implementation

CISA designed the Cybersecurity Performance Goals (CPGs) for organizations to apply across all aspects of their environment. However, it is important to note that the guidance regarding Cost, Impact, and Ease of Implementation—particularly as outlined in the stated goals—primarily applies to IT infrastructure. This means that the considerations and recommendations presented in these goals do not necessarily extend to OT systems or other non-IT environments within an organization.

<table>
<tr><th colspan="3">Cost</th></tr>
<tr><td><b>Low</b> cost is less than 5% of an organization’s annual security budget.</td><td><b>Moderate</b> cost is between 5% and 15% of an organization’s annual security budget.</td><td><b>High</b> cost is greater than 15% of an organization’s annual security budget.</td></tr>
<tr><td colspan="3"><b>Description:</b> The financial cost to implement, maintain, and dispose of (the assets supporting) the capability goal.
• Consider costs during the first year of implementation and recurring costs over years 2-3+ to maintain the service.
• Assess costs as a percentage of security spend.</td></tr>
<tr><td colspan="3"><b>Cost-Benefit Analysis</b></td></tr>
<tr><td colspan="3">Conduct a cost-benefit analysis (CBA) for any CPG that may not be implemented. This is especially important for CPGs with high costs ($$$) that may seem harder to justify. A CBA, comparing quantified benefits and costs, may help decision-makers justify the cybersecurity investment with more objectively defensible information.

<b>Costs</b> – Consider costs for the CPG over its life—hardware, software, and level of effort (support time).

<b>Benefits</b> – Consider potential impacts, in financial terms, averted. In particular:
• Productivity. Consider how downtime would affect operations and any associated financial impacts, such as revenue losses.
• Response. Consider the size of the incident response team, the time spent in response, and any management review time.
• Replacement costs. Consider any expenditures on new equipment required to replace existing solutions.
• Other factors. Consider potential competitive advantage and beneficial reputation, as warranted.</td></tr>
</table>

<table>
<tr><th colspan="3">Impact</th></tr>
<tr><td><b>Low</b> impact prevents limited adverse effects on an organization’s operations, assets, or individuals. “Limited adverse effects” means that the organization can continue to support the organization’s mission.</td><td><b>Moderate</b> impact prevents serious adverse effects on an organization’s operations, assets, or individuals. “Serious adverse effects” means that the organization will be unable to support some parts of the organization’s mission.</td><td><b>High</b> impact prevents severe or catastrophic adverse effects on an organization’s operations, assets, or individuals. “Severe or catastrophic adverse effects” means that the organization will be unable to support the organization’s mission.</td></tr>
<tr><td colspan="3"><b>Description:</b> A measure of the likely protection offered by the capability goal against potential harms to the organization, individuals, and the environment.

• Assess the protection offered as the reduction of potential losses due to stronger resilience and protection of confidentiality, integrity, and availability (CIA) provided by the capability goal.
• At a qualitative level, CPG impact definitions mirror the NIST Risk Management Framework system categorization (Low, Moderate, High) for the relevant CIA factor(s) affected by the CPG.

This measure considers traditional losses (direct and indirect) and harms to the organization (e.g., mission, assets, reputation), individuals (e.g., health, safety), and ecosystems.</td></tr>
<tr><th colspan="3">Ease of Implementation</th></tr>
<tr><td><b>Simple</b> projects/systems can be implemented within a few months with minimal technical expertise.</td><td><b>Moderate</b> projects/systems can be implemented within 4 to 8 months and require moderate technical expertise or management involvement.</td><td><b>Complex</b> projects/systems generally take closer to a year or longer to implement and require significant technical expertise, coordination, and management involvement.</td></tr>
<tr><td colspan="3"><b>Description:</b> A rating of difficulty to implement and manage the capability goal.

The rating (Simple, Moderate, Complex) assesses how clear, actionable, and reasonably straightforward CPG implementation and management is.

The focus is on the level of technical expertise and time investment required to implement the CPG.</td></tr>
</table>

GOVERN

1.A– ESTABLISH CYBERSECURITY RESPONSIBILITIES

OUTCOME

Roles, responsibilities, and authorities related to the organization's cybersecurity program are established, communicated, enforced, and aligned within the organization and external partners.

RISK ADDRESSED

Lack of sufficient cybersecurity accountability, investment, or effectiveness.

SCOPE

C-suite personnel, critical section leadership, physical and cybersecurity personnel, third-party contractors, vendors, and suppliers.

RECOMMENDED ACTION

All roles and responsibilities involving cybersecurity should be documented in an organization's cybersecurity policy.

Roles and responsibilities related to the cybersecurity policy and program are distributed across the organization. Third-party contractors can also be involved to assist with these activities.

Ensure that legal and regulatory requirements regarding cybersecurity, including privacy, are implemented and managed.

OT: Establish and maintain continuous collaboration between information technology (IT) and operational technology (OT) teams in order to streamline processes, enhance security measures, and boost operational effectiveness.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
GV.RR-02	Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: PM-2, PM-13, PM-19, PM-23, PM-24, PM-29
SP 800-82 Rev 3: PS-2

SUPPORT RESOURCES

Cyber Storm National Cybersecurity Exercise
Executive Cybersecurity Leadership

1.B– MANAGE CYBERSECURITY OVERSIGHT

OUTCOME

The organization's cybersecurity risk management strategy, expectations, and policies are established.

RISK ADDRESSED

Insufficient cybersecurity policies and procedures/practices that can manage cybersecurity risk for the organization's technologies and processes.

SCOPE

Organization-wide.

RECOMMENDED ACTION

Policies for managing the cybersecurity program are reviewed at least annually, updated when changes are applied, communicated, and enforced to reflect changes in requirements, risks, threats, technology, and organizational mission. Policies are established based on the organization and its cybersecurity strategy, and priorities are communicated and enforced. It is recommended that organizational governance encompass the policies, procedures, and processes necessary to manage the organization's regulatory, legal, risk, environmental, and operational obligations.

OT: OT-specific policies and procedures should consider the limitations of the existing IT cybersecurity program to identify priorities for critical operational functions, OT-specific security concerns, and compensating controls.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
GV.OV-03	Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: PM-4, PM-6, RA-7, SR-6
SP 800-82 Rev 3: RA-1

SUPPORT RESOURCES

CISA Cybersecurity Awareness Program
Cybersecurity Best Practices

1.C– MAINTAIN INCIDENT RESPONSE PLANS

OUTCOME

Identify improvements by practicing cybersecurity and incident response (IR) plans to maintain and update the organization’s cybersecurity program.

RISK ADDRESSED

Inability to quickly and effectively isolate, contain, eradicate, remediate, and communicate about cybersecurity incidents.

SCOPE

Organization-wide.

RECOMMENDED ACTION

Organizations develop, maintain, update, and regularly exercise IR plans for common and organizationally specific (e.g., by sector, locality) threat scenarios and tactics, techniques, and procedures (TTPs). Ensure drills are realistic and include all relevant stakeholders. IR plans should be reviewed and drilled, at a minimum, on an annual basis.

OT: OT IR plans account for specific safety and containment considerations, which differ from existing IT plans and priorities.

NIST CSF 2.0 REFERENCE(S)

ID.IM-02, ID.IM-04

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, SR-2, CA-2, CA-5, CA-7, CA-8, CP-2, CP-4, IR-3, IR-4, IR-8, PL-2, PM-4, PM-31, RA-3, RA-5, RA-7, SA-8, SA-11, SI-2, SI-4, SR-5
SP 800-82 Rev 3: CA-2, CA-5, CP-1, CP-2, CP-4, CP-10, IR-1, IR-8, SA-11, RA-3, SR-6

SUPPORT RESOURCES

CISA Tabletop Exercise Packages
Incident Response Plan (IRP) Basics
Critical Infrastructure Exercises Support
Develop an Incident Response Capability

1.D– SUPPLY CHAIN INCIDENT REPORTING & VULNERABILITY DISCLOSURE

OUTCOME

Organizations more rapidly learn about and respond to known incidents or breaches across vendors and service providers.

RISK ADDRESSED

Insufficient cybersecurity supply chain risk management (C-SCRM) practices that cannot securely support the organization's technologies and processes.

SCOPE

Third-party vendors and service providers.

RECOMMENDED ACTION

Procurement documents and contracts, such as service-level agreements (SLAs), stipulate that vendors and/or service providers notify the procuring customer of security incidents and vulnerabilities within a risk-informed time frame as determined by the organization.

OT: Organizations with OT assets need to document and track serial numbers, checksums, digital certificates/signatures, or other identifying features that can enable them to verify the authenticity of vendor-provided OT hardware, software, and firmware.

NIST CSF 2.0 REFERENCE(S)

GV.SC-01, GV.SC-05

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	Moderate	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: SA-4, SA-9, PM-30, SR-2, SR-3, SR-5, SR-6, SR-10
SP 800-82 Rev 3: PL-1

SUPPORT RESOURCES

Information and Communications Technology Supply Chain Security
Supply Chain Risk Management (SCRM) in a Connected World

1.E–

MANAGE RISKS FROM MANAGED SERVICE PROVIDERS

OUTCOME

The risks posed by a managed service provider (MSP) are identified, recorded, assessed, prioritized, monitored, and updated over the course of the relationship.

RISK ADDRESSED

Adversaries can exploit vulnerabilities by abusing trusted third-party relationships.

SCOPE

Service providers that remotely manage an organization's IT and/or OT infrastructure, cybersecurity processes, and/or other related business operations.

RECOMMENDED ACTION

Develop and maintain an understanding of the services, including the security products provided by MSPs. Understand contractual agreements and proactively address any security gaps that fall outside the scope of the contract. For example: Contracts should detail how and when MSPs notify the customer of an incident affecting the customer's environment.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
GV.SC-07	Moderate	Moderate	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: RA-9, SA-4, SA-9, SR-3, SR-6
SP 800-82 Rev 3: RA-9, SA-4, SR-1, SR-2, SR-3, SR-6

SUPPORT RESOURCES

Protecting Against Cyber Threats to Managed Service Providers and their Customers
Risk Considerations for Managed Service Provider Customers

IDENTIFY

2.A– MANAGE ORGANIZATIONAL ASSETS

OUTCOME

A maintained asset inventory to improve cybersecurity resilience by reducing downtime, aiding recovery, bolstering defenses, and improving preparedness.

RISK ADDRESSED

Adversaries might use computer accessories, networking hardware, or other devices as entry points to infiltrate systems or networks.

SCOPE

Data, hardware, software, systems, facilities, personnel.

RECOMMENDED ACTION

Maintain a regularly updated inventory of all organizational assets (i.e., data, hardware, software, systems, facilities, and personnel).

IT and OT assets determined to be critical for business or operational functions should be updated on a more frequent basis.

NIST CSF 2.0 REFERENCE(S)

ID.AM-01

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CM-8, PM-5
SP 800-82 Rev 3: CM-8

SUPPORT RESOURCES

Asset Inventory for OT
Asset Management
CISA Insights: Secure High Value Assets (HVAs)

2.B– MITIGATE KNOWN VULNERABILITIES

OUTCOME

Reduced likelihood of threat actors exploiting known vulnerabilities to breach organizational networks.

RISK ADDRESSED

Adversaries frequently target unpatched and misconfigured systems, particularly those exposed to the internet. Adversaries often leverage software vulnerabilities, temporary malfunctions, or configuration errors to gain initial access to a network.

SCOPE

All organizational assets, to include those that face the internet.

RECOMMENDED ACTION

Implement a vulnerability management program to patch and mitigate misconfigured software in a timely manner.

Monitor risk response progress through tools such as plan of action and milestones (POA&M), risk registers, and risk detail reports.

Document potential risks of proposed changes and provide rollback guidance. Assign responsibilities and ensure procedures are followed for processing and responding to cybersecurity threats, vulnerabilities, or incident disclosures from various stakeholders. Incorporate compensating security controls (e.g., defense in depth) to address legacy systems, where possible.

OT: For assets where patching is either not possible or may substantially compromise availability or safety, compensating controls are applied (e.g., segmentation, monitoring) and recorded. Sufficient controls either make the asset inaccessible from the public internet or reduce the ability of threat actors to exploit the vulnerabilities in these assets.

NIST CSF 2.0 REFERENCE(S)

ID.RA-01, ID.RA-06, ID.RA-08

COST	IMPACT	EASE OF IMPLEMENTATION
High	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CA-2, CA-7, CA-8, PM-9, PM-18, PM-30, RA-3, RA-5, RA-7, SA-11(02), SA-15(07), SA-15(08), SI-4, SI-5
SP 800-82 Rev 3: CA-1, CA-2, CA-5, RA-3, RA-7, SA-11, SI-2, SI-3, SI-5

SUPPORT RESOURCES

Known Exploited Vulnerabilities Catalog
CISA Cyber Hygiene Services
Think Twice Before Putting Off Updates!
Understanding Patches and Software Updates
ICS Recommended Practices

2.C– OBTAIN INDEPENDENT VALIDATION OF CYBERSECURITY CONTROLS

OUTCOME

Validate that implemented security controls are properly configured and working as intended.

RISK ADDRESSED

Reduce the risk of gaps in cyber defenses or overconfidence in existing protections.

SCOPE

Organizational assets and networks.

RECOMMENDED ACTION

Organizations regularly engage third-party cybersecurity experts to validate their defenses through various exercises, such as penetration tests, bug bounties, incident simulations, and table-top exercises. These tests, both announced and unannounced, assess the ability of adversaries to infiltrate and move laterally within the network, targeting critical systems. Ensure findings from these tests are addressed.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
ID.RA-01, ID.RA-03	High	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CA-2, CA-7, CA-8, PM-12, PM-16, RA-3, RA-5, SA-11(02), SA-15(07), SA-15(08), SI-4, SI-5
SP 800-82 Rev 3: AT-2(2), CA-1, CA-2, CA-5, RA-3, SA-11, SI-2, SI-3, SI-5

SUPPORT RESOURCES

CISA Cyber Hygiene Services
Cybersecurity Performance Goals (CPG) Assessment Training
Risk and Vulnerability Assessments

2.D– MAINTAIN VULNERABILITY DISCLOSURE/REPORTING PROCESS

OUTCOME

Organizations learn about vulnerabilities or weaknesses more rapidly.

RISK ADDRESSED

Reporting known security vulnerabilities in a company's software, networks, devices, and systems directly to the organization allows them to address and mitigate these vulnerabilities before adversaries can exploit them.

SCOPE

All public-facing assets and web domains.

RECOMMENDED ACTION

Organizations maintain a public, easily discoverable method for individuals to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity.

Individuals who identify and report vulnerabilities discovered in good faith should be protected under safe harbor rules. Safe harbor rules are provisions in law that protect individuals or entities from penalties under certain conditions.

Security.txt files that conform with the recommendations in RFC 9116 are one commonly utilized standard to streamline vulnerability notifications. This should be applied to all public-facing web domains.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
ID.RA-08	Low	Low	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: RA-5
SP 800-82 Rev 3: RA-5, SI-2, SI-3, SI-5

SUPPORT RESOURCES

CISA Coordinated Vulnerability Disclosure Program
Vulnerability Disclosure Policy Template
security.txt: A Simple File with Big Value

2.E–

DOCUMENT NETWORK TOPOLOGY

OUTCOME

Respond to incidents and maintain service continuity more efficiently and effectively.

RECOMMENDED ACTION

Organizations maintain accurate documentation describing current network topology and relevant information across all IT and OT networks. Network reviews should be performed and tracked on an annual basis and documentation updated when network topology changes are made.

RISK ADDRESSED

Incomplete or inaccurate understanding of network topology inhibits effective incident response and recovery.

SCOPE

Organizational networks.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
PR.PS-01, ID.AM-03	Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
SP 800-82 Rev 3: CM-1, CM-9

SUPPORT RESOURCES

Introduction to Network Diagramming
Cybersecurity Best Practices for Smart Cities

3.A CHANGE DEFAULT PASSWORDS

OUTCOME

Prevent threat actors from using default passwords to achieve initial access and move laterally in a network.

RISK ADDRESSED

Adversaries might acquire and exploit default account credentials to gain initial access, maintain persistence, escalate privileges, or evade defenses.

SCOPE

Password-protected newly acquired and legacy IT and OT assets.

RECOMMENDED ACTION

Implement an organization-wide policy that requires changing default manufacturer passwords for all hardware, software, and firmware before connecting them to any internal or external network. This includes IT assets used in OT, such as OT administration web pages.

If changing default passwords is not feasible (e.g., due to hard-coded passwords in control systems), document and implement appropriate compensating security controls and monitor logs for network traffic and login attempts on these devices.

OT: Change default passwords on existing OT systems and establish a policy for changing default credentials on all new or future devices. This will reduce potential risk in the future if vulnerabilities change.

NIST CSF 2.0 REFERENCE(S)

PR.AA-01

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Simple

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

SUPPORT RESOURCES

How Manufacturers Can Protect Customers by Eliminating Default Passwords
Risks of Default Passwords on the Internet

3.B ESTABLISH MINIMUM PASSWORD STRENGTH

OUTCOME

Organizational passwords are harder for threat actors to guess or crack.

RISK ADDRESSED

Adversaries use brute force techniques to crack passwords when unknown or hashes are obtained. They systematically guess using repetitive methods, either interacting with services to validate credentials or working offline with acquired data.

SCOPE

User account passwords.

RECOMMENDED ACTION

Organizations have a system-enforced policy to establish a minimum password strength, to include a password length of 16 or more characters for all password-protected IT assets and all OT assets, when technically feasible. Organizations should consider leveraging passphrases and password managers to make it easier for users to maintain sufficiently long passwords. In instances where minimum password lengths are not technically feasible, compensating controls are applied and recorded, and all login attempts to those assets are logged. Assets that cannot support passwords of sufficient strength are prioritized for upgrade or replacement.

NIST CSF 2.0 REFERENCE(S)

PR.AA-01

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Simple

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

SUPPORT RESOURCES

Use Strong Passwords
Require Strong Passwords

3.C–

CREATE UNIQUE CREDENTIALS

OUTCOME

Adversaries are unable to reuse compromised credentials to move laterally across the organization, particularly between IT and OT networks.

RISK ADDRESSED

Adversaries can obtain and exploit account credentials to gain access, maintain persistence, escalate privileges, or evade defenses. These credentials can bypass network access controls for continuous access to remote systems and external services.

SCOPE

User accounts.

RECOMMENDED ACTION

Organizations create distinct and separate credentials for similar services and asset access across IT and OT networks. Users refrain from reusing passwords for their accounts, applications, and services. Additionally, system administrators and service/machine accounts have unique passwords credentials that differ from those of regular user accounts.

No universal non-person entity (NPE) account passwords should be deployed. If NPE devices are used, leverage different passwords for each.

Role-based accounts for IT and OT systems are utilized when possible.

NIST CSF 2.0 REFERENCE(S)

PR.AA-01

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Simple

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

SUPPORT RESOURCES

Cyb3R_Sm@rT!: Use a Password Manager
Using Rigorous Credential Control

3.D–

REVOKE CREDENTIALS FOR DEPARTING STAFF

OUTCOME

Prevent unauthorized access to organizational accounts or resources by former staff.

RISK ADDRESSED

Adversaries can exploit inactive accounts of former staff to evade detection.

SCOPE

Departing staff, who may include contractors, vendors, etc.

RECOMMENDED ACTION

Organizations should have a defined and enforced administrative process to off board staff (e.g., personnel, contractors, vendors). This process should include the return of all physical tokens and/or badges and the revocation of all access to systems and facilities.

Review user access and disable accounts when inactive for a specified period (e.g., 30 days). Ideally this review is conducted using an automated process and preset policies implemented via script or platform feature.

NIST CSF 2.0 REFERENCE(S)

PR.AA-01

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

SUPPORT RESOURCES

Managing Risk of Adverse/Involuntary Employee Separations

3.E–

MONITOR UNSUCCESSFUL (AUTOMATED) LOGIN ATTEMPTS

OUTCOME

Protect organizations from automated, credential-based attacks.

RISK ADDRESSED

Adversaries might acquire and exploit default account credentials to gain access, maintain persistence, escalate privileges, or evade defenses.

SCOPE

Password-protected newly acquired and legacy IT and OT assets.

RECOMMENDED ACTION

All unsuccessful logins are captured and logged as directed by the organization's security policy. Security personnel are notified (e.g., by an alert) after a specific number of consecutive unsuccessful login attempts in a short period and a deviation from normal user behavior. This alert is logged and stored in the relevant security or ticketing system for retroactive analysis.

NIST CSF 2.0 REFERENCE(S)

PR.AA-01

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AC-2, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

SUPPORT RESOURCES

Stop Ransomware Guide
Brute Force Attacks Conducted by Cyber Actors

3.F–

IMPLEMENT MULTIFACTOR AUTHENTICATION (MFA)

OUTCOME

Add a critical, additional layer of security to protect assets' accounts.

RISK ADDRESSED

Adversaries without prior knowledge of legitimate credentials might try commonly used passwords across various accounts to gain access. They might also systematically guess passwords using repetitive or iterative methods.

SCOPE

Organizational assets with remote access, such as workstations and human-machine interfaces (HMIs), where safe and technically feasible.

RECOMMENDED ACTION

Organizations require MFA to access assets using the strongest available method, if MFA is available for that asset.

MFA options sorted by strength, high to low, are as follows:

1. Phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure [PKI]-based—see CISA guidance in "Support Resources").

2. If phishing-resistant MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching).

3. MFA via short message service (SMS) or voice is only used when no other options are possible.

IT: All IT accounts leverage MFA to access organizational resources. Prioritize accounts with highest risk, such as privileged administrative accounts for key IT systems.

OT: MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible HMIs when available. If MFA is not available, remove remote access, introduce additional segmentation steps, and prioritize credential management.

NIST CSF 2.0 REFERENCE(S)

PR.AA-03

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-7, AC-12, IA-2, IA-3, IA-5, IA-7, IA-8, IA-9, IA-10, IA-11
SP 800-82 Rev 3: IA-2, IA-3, IA-8

SUPPORT RESOURCES

Implementing Phishing-Resistant MFA
Protect Our World with MFA

3.G ADMINISTRATORS MAINTAIN SEPARATE USER AND PRIVILEGED ACCOUNTS

OUTCOME

Make it harder for threat actors to gain access to administrator or privileged accounts, even if common user accounts are compromised.

RISK ADDRESSED

Adversaries might obtain and exploit credentials from existing accounts for initial access, persistence, privilege escalation, or defense evasion. These compromised credentials can bypass network access controls and provide continuous access to remote systems and external services.

SCOPE

Organizational assets, where safe and technically feasible.

RECOMMENDED ACTION

User accounts do not have administrator privileges. Administrators maintain separate user accounts for activities unrelated to their admin role, such as business email and web browsing. Privileges are re-evaluated on a recurring basis to validate continued need for a given set of permissions.

Separation of duties is maintained by distributing responsibilities across multiple individuals or roles to reduce the risk of unauthorized actions, errors, or fraud.

NIST CSF 2.0 REFERENCE(S)

PR.AA-05

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Simple

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AC-2, AC-3, AC-5, AC-6, AC-10, AC-16, AC-17, AC-18, AC-19, AC-24, IA-13
SP 800-82 Rev 3: AC-1, AC-5, AC-6, IA-1, IA-2, IA-3, IA-8, PS-2

SUPPORT RESOURCES

Top Ten Cybersecurity Misconfigurations
Enhancing Cyber Resilience: Insights from CISA Red Team
NIST - Separation of Duty

3.H IMPLEMENT THE PRINCIPLES OF LEAST PRIVILEGE

OUTCOME

Minimizes unauthorized access to systems, data, and processes, reduces human error, and prevents malicious actions; helping ensure the organization's sensitive information and critical assets remain protected.

RISK ADDRESSED

Unauthorized access to network resources and the potential for adversaries to move across systems undetected, compromising sensitive data and critical systems.

SCOPE

All organizational accounts.

RECOMMENDED ACTION

All user accounts, system roles, and processes operate with the minimum privileges necessary to perform their tasks.

Perform quarterly reviews of access permissions and role assignments to verify compliance with established policies.

NIST CSF 2.0 REFERENCE(S)

PR.AA-05

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Simple

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-5, AC-6, SA-8(14), SA-17(7), SC-3
SP 800-82 Rev 3: AC-5, AC-6

SUPPORT RESOURCES

Weak Security Controls and Practices Routinely Exploited
Enhanced Visibility and Hardening Guidance
Principle of Least Privilege

3.I–

IMPLEMENT LOGICAL/PHYSICAL NETWORK SEGMENTATION

OUTCOME

Limiting the impact(s) of a potential breach and preventing adversaries from accessing sensitive data, spaces, and/or critical infrastructure.

RISK ADDRESSED

If a network is compromised by an unauthorized user, a securely segregated network can contain malicious occurrences.

SCOPE

Organizational assets, where safe and technically feasible.

RECOMMENDED ACTION

Routers are placed between networks to create boundaries, increase the number of broadcast domains, and effectively filter users' broadcast traffic. These boundaries can be used to contain security breaches by restricting traffic to separate segments and can even shut down segments of the network during an intrusion, restricting adversary access.

OT: When applicable, physically segment OT enclaves (e.g., data diodes).

NIST CSF 2.0 REFERENCE(S)

PR.IR-01, DE.CM-01

COST	IMPACT	EASE OF IMPLEMENTATION
High	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-12, CA-7, CM-3, SC-4, SC-5, SC-7, SI-4
SP 800-82 Rev 3: AU-1, AU-2, SA-8, SC-1, SC-7(18), SI-1, SI-4, PL-8

SUPPORT RESOURCES

Layering Network Security Through Segmentation

3.J–

IMPLEMENT CYBERSECURITY TRAINING

OUTCOME

Organizational users learn and perform more secure behaviors.

RISK ADDRESSED

Train users on recognizing access or manipulation attempts by adversaries to lower the risk of successful spear phishing, social engineering, and other techniques that involve user interaction.

SCOPE

All employees, contractors, partners, suppliers, providers, and other users of the organization's non-public resources.

RECOMMENDED ACTION

New employees receive initial cybersecurity training prior to accessing computer systems.

Provide at least annual cybersecurity training for all organizational users to train personnel in recognizing social engineering attempts and other common attacks, reporting attacks and suspicious activity, complying with acceptable use policies, and performing basic cyber hygiene tasks (e.g., choosing passwords, protecting credentials).

Identify the specialized roles within the organization that require additional cybersecurity training, such as physical and cybersecurity personnel, system administrators, finance personnel, senior leadership, and anyone with access to business-critical data. Provide role-based cybersecurity training to all those in specialized roles, including contractors, partners, suppliers, and other third parties.

OT: Personnel should receive security awareness and training for the OT environment. In addition, organizations should identify, document, and train all personnel who have significant OT roles and responsibilities.

NIST CSF 2.0 REFERENCE(S)

PR.AT-01, PR.AT-02

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AT-2, AT-3
SP 800-82 Rev 3: AT-2, AT-3

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Moderate

SUPPORT RESOURCES

CISA Training
Cybersecurity Training & Exercises

3.K–

UTILIZE STRONG ENCRYPTION

OUTCOME

Encryption is deployed to maintain confidentiality and integrity of sensitive data across the organization's network to protect from unauthorized access.

RISK ADDRESSED

Adversaries can position themselves between networked devices to enable network sniffing and data manipulation, or to steal operational data from environments for personal gain or future operations.

SCOPE

Passwords, credentials, secrets, and other sensitive or controlled information.

NIST CSF 2.0 REFERENCE(S)

PR.DS-01, PR.DS-02, PR.DS-10

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-9, AU-13, AU-16, CA-3, CP-9, MP-8, SA-8, SC-4, SC-7, SC-8, SC-11, SC-12, SC-13, SC-16, SC-24, SC-28, SC-32, SC-39, SC-40, SC-43, SI-3, SI-4, SI-7, SI-10, SI-16
SP 800-82 Rev 3: AC-6, CM-2, CM-6, MP-1, PL-10, SA-8, SC-8, SC-13, SC-28

RECOMMENDED ACTION

Use encryption, digital signatures, and cryptographic hashes to protect the confidentiality and integrity of network communications.

Identify critical electronic file types and data to protect while in transit and at rest. This may include personally identifiable information and sensitive, proprietary or trade secret information (e.g., PLC program code, robot programs, computer-aided drafting [CAD] or computer-aided manufacturing [MAC] files, operating manuals and documentation, electrical diagrams, network diagrams, historical production data).

Sensitive data, including passwords, are not electronically stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager.

OT: Use encryption for external connections and where latency issues would not result in an impact to operations.

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Complex

SUPPORT RESOURCES

How to Protect the Data that is Stored on Your Devices

3.L–

ENABLE EMAIL SECURITY

OUTCOME

Reduce risk from common email-based threats, such as spoofing, phishing, and interception.

RISK ADDRESSED

Adversaries might send victims emails with malicious attachments or links, aiming to run harmful code on their systems. They can also conduct phishing through third-party services like social media platforms.

SCOPE

All organizational email infrastructure.

NIST CSF 2.0 REFERENCE(S)

PR.DS-01, PR.DS-02, PR.DS-10

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-9, AU-13, AU-16, CA-3, CP-9, MP-8, SA-8, SC-4, SC-7, SC-8, SC-11, SC-12, SC-13, SC-16, SC-24, SC-28, SC-32, SC-39, SC-40, SC-43, SI-3, SI-4, SI-7, SI-10, SI-16
SP 800-82 Rev 3: AC-6, CM-2, CM-6, MP-1, PL-10, SA-8, SC-8, SC-13, SC-28

RECOMMENDED ACTION

On all corporate email infrastructure (1) STARTTLS is enabled, (2) Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) are enabled, and (3) Domain-based Message Authentication, Reporting, and Conformance (DMARC) is enabled and set to "reject."

COST	IMPACT	EASE OF IMPLEMENTATION
Low	High	Moderate

SUPPORT RESOURCES

BOD 18-01: Enhance Email and Web Security
CISA Insights - Enhance Email & Web Security

3.M

DISABLE AUTORUN & MACROS BY DEFAULT

OUTCOME

Reduce the risk from embedded macros and similar executable code.

RISK ADDRESSED

Adversaries rely on users to open malicious files to execute code. Social engineering tactics could be used to convince users to open such files.

SCOPE

All organizational assets.

RECOMMENDED ACTION

A system-enforced policy that disables macros, or similar embedded code, by default on all devices to prevent automatic execution of code or applications.

If macros must be enabled in specific circumstances, establish a policy for authorized users to request that macros are enabled on specific assets.

Autorun, or AutoPlay, should also be disabled by default to prevent unintentional code execution from sources such as USB or optical drives.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
PR.PS-01, ID.RA-07	Low	Moderate	Simple

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CA-7, CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11
SP 800-82 Rev 3: CM-1, CM-3, CM-4, CM-5, CM-9

SUPPORT RESOURCES

Using Caution with USB Drives
Disable AutoRun Properly

3.N

ESTABLISH CHANGE MANAGEMENT PROCESSES

OUTCOME

Policies and procedures exist to manage system changes and configurations.

RISK ADDRESSED

Delayed, insufficient, or incomplete ability to maintain or restore functionality of critical devices and service operations.

SCOPE

Organizational assets.

RECOMMENDED ACTION

Implement policies and processes to develop, document, and maintain secure change management for technology platforms and enforce configuration restrictions to prevent unauthorized changes.

Technical configuration change control processes are in place, prohibiting unauthorized changes unless approved. Test and document proposed changes in a non-production environment and analyze potential security impacts before implementation.

OT: Implement limited functionality by permitting only specific functions, protocols, and services necessary for OT operations.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
PR.PS-01, PR.PS-02, PR.PS-03	Moderate	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CM-1, CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-8, CM-9, CM-10, CM-11, MA-3(06), SA-10(01), SA-10(03), SI-2, SI-7, SC-03(01), SC-39(01), SC-49, SC-51
SP 800-82 Rev 3: CM-1, CM-9, MA-1, MA-2, MA-6, SA-3, SA-22, SI-2, SI-3

SUPPORT RESOURCES

Configuration and Change Management
Importance of Configuration and Change Management to Security

3.O–

MAINTAIN SYSTEM BACKUPS & RESTORATION ABILITY

OUTCOME

Organizations reduce data loss and service disruption risks while efficiently managing, responding to, and recovering from incidents to maintain continuous service delivery.

RISK ADDRESSED

Adversaries can disrupt critical systems to halt the delivery of products or services. They can delete data and disable recovery services, preventing system recovery. Adversaries may turn off services designed to aid in recovering a corrupted system.

SCOPE

Organizational assets necessary for business operations.

NIST CSF 2.0 REFERENCE(S)

PR.IR-01, DE.CM-01

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-2, AC-3, AC-4, AU-12, CA-7, CM-3, SC-4, SC-5, SC-7, SI-4
SP 800-82 Rev 3: AU-1, AU-2, SA-8, SC-1, SC-7(18), SI-1, SI-4, PL-8

RECOMMENDED ACTION

Develop a list of all maintained backups, including installation media, license keys, configuration information, and backup retention period of the information.

Back up critical operations systems in near-real-time, and frequently back up all systems necessary for operations on a regular schedule consistent with the needs of the organization.

Securely store backups offsite and offline. Test backups and recovery on a recurring basis, no less than once per year.

Before initiating restoration, validate the integrity of backups and other assets intended for restoration. This verification process is to ensure that data is intact, accurate, and reliable, minimizing the risk of data corruption during the restoration process.

Check restoration assets for indicators of compromise, file corruption, and other integrity issues before use.

Regularly test backup information to verify media reliability and information integrity.

OT: Stored information for OT assets includes, at a minimum, device configurations, roles, engineering drawings, and tools.

COST	IMPACT	EASE OF IMPLEMENTATION
High	High	Moderate

SUPPORT RESOURCES

CISA Stop Ransomware Guide
Cyber Guidance for Small Businesses

3.P–

MAINTAIN HARDWARE & SOFTWARE APPROVAL PROCESS

OUTCOME

Increase visibility into deployed technology assets and reduce the likelihood of breach by users installing unapproved hardware, firmware, or software.

RISK ADDRESSED

Adversaries can manipulate products or delivery mechanisms before they reach final users and attempt data or system compromise. They can target devices that move across industrial control systems and production networks.

SCOPE

Organizational assets.

NIST CSF 2.0 REFERENCE(S)

PR.PS-02, PR.PS-03, ID.RA-07

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CA-7, CM-3, CM-4, CM-7(09), CM-11, MA-3(06), SA-10(01), SC-3(01), SC-39(01), SC-49, SC-51, SI-2, SI-7
SP 800-82 Rev 3: CM-3, CM-4, CM-5, MA-1, MA-2, MA-6, SA-3, SA-22, SI-2, SI-3

RECOMMENDED ACTION

Implement an administrative policy and process that requires review, testing, and approval before new hardware, firmware, or software is installed or deployed.

Organizations maintain a list of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible.

OT: Consider additional requirements for organizations with OT environments when deploying patches and updates. This includes testing and validation to ensure they do not impact operational capabilities or safety.

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Moderate

SUPPORT RESOURCES

Securing the Software Supply Chain

3.Q– MAINTAIN LOG COLLECTION & STORAGE

OUTCOME

Enhance visibility to detect and respond to cyber incidents while ensuring security logs are protected from unauthorized access and tampering.

RISK ADDRESSED

Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents.

SCOPE

Organizational assets on all assets, where safe and technically feasible.

RECOMMENDED ACTION

Administrative and security-focused logs (e.g., operating systems, applications, and services; intrusion detection systems/intrusion prevention systems; firewalls; data loss prevention; virtual private networks) are collected and stored for use in both detection and incident response activities (e.g., forensics).

Logs are stored in a central system, such as a security information and event management tool or central database, and can only be accessed or modified by authorized and authenticated users. Logs are stored for a duration informed by risk or pertinent regulatory guidelines.

Security teams are notified when a critical log function is disabled.

OT: For OT assets where logs are non-standard or not available, network traffic and communications between those assets and other assets is collected.

NIST CSF 2.0 REFERENCE(S)

PR.PS-04

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AU-2, AU-3, AU-6, AU-7, AU-11, AU-12
SP 800-82 Rev 3: AU-1, AU-3, SI-4

SUPPORT RESOURCES

Best Practices for Event Logging and Threat Detection
Guide to Computer Security Log Management
Improving Investigative and Remediation Capabilities

3.R– PROHIBIT CONNECTION OF UNAUTHORIZED DEVICES

OUTCOME

Prevent malicious actors from achieving initial access or data exfiltration via unauthorized portable media devices.

RISK ADDRESSED

Adversaries might infiltrate systems, including disconnected or air-gapped networks, by copying malware to removable media such as USB drives.

SCOPE

Organizational assets.

RECOMMENDED ACTION

Organizations maintain policies and processes to ensure that unauthorized media and hardware are not connected to IT and OT assets, such as limiting use of USB devices and removable media.

OT: When feasible, establish procedures to remove, disable, or otherwise secure physical ports to prevent the connection of unauthorized devices or establish procedures for granting access through approved exceptions.

NIST CSF 2.0 REFERENCE(S)

PR.DS-01

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: CA-3, CP-9, MP-8, SC-4, SC-7, SC-12, SC-13, SC-28, SC-32, SC-39, SC-43, SI-3, SI-4, SI-7
SP 800-82 Rev 3: MP-1, SC-8(1), SC-13, SC-28

SUPPORT RESOURCES

Using Caution with USB Drives
Proposed Security Requirements for Restricted Transactions

3.S–

SECURE INTERNET-FACING DEVICES

OUTCOME

Unauthorized users cannot gain an initial system foothold by exploiting known weaknesses in internet-facing assets.

RISK ADDRESSED

Adversaries might exploit weaknesses in internet-facing hosts or systems to gain initial network access, targeting software bugs, temporary glitches, or misconfigurations.

SCOPE

Organizational assets on the public internet.

RECOMMENDED ACTION

Minimize internet-facing assets whenever possible. Prioritize keeping software current with timely patches and updates. If unable to apply updates, consider removing that asset, or implement compensating controls to prevent common forms of exploitation. These controls may include network segmentation or firewalls.

All operating system applications, software and network protocols that are not necessary for mission-critical applications are disabled on internet-facing assets.

Network management interfaces (NMIs) should never be exposed to the public internet and should only be accessible from within enterprise networks.

Logically segment enterprise networks and production networks, including cloud-based platforms, according to trust boundaries and platform types (e.g., IT, IoT, OT, mobile, guests), and only permit required communications between segments.

NIST CSF 2.0 REFERENCE(S)

PR.IR-01

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-3, AC-4, SC-4, SC-5, SC-7
SP 800-82 Rev3: PL-8, SA-8, SC-1, SC-7(18), SI-1

SUPPORT RESOURCES

Remediate Vulnerabilities for Internet-Accessible Systems
Internet Exposure Reduction Guidance
Mitigating the Risk from Internet-Exposed Management Interfaces

DETECT

4.A– ESTABLISH MALICIOUS CODE DETECTION

OUTCOME

Enables early threat identification, strengthens system integrity, provides insights for faster remediation, and minimizes downtime.

RISK ADDRESSED

Malicious software can involve payloads, droppers, backdoors, etc. Adversaries use malware to control remote machines, evade defenses, and execute post-compromise actions.

SCOPE

Organization-wide.

RECOMMENDED ACTION

Implement signature-based mechanisms (relying on known patterns or signatures of malicious code used by antivirus software to identify and block threats) and non-signature-based mechanisms (focusing behavior, heuristics, or anomalies) to detect and eradicate malicious code at system endpoints. Ensure antivirus software is updated, active, and configured to automatically scan emails and removable media (e.g., flash drives) for ransomware and other malware.

OT: Using antivirus software with OT devices may require special practices, including compatibility checks, change management, and performance impact metrics. These practices should be employed to test new signatures and new versions of malicious code protection solutions.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
DE.CM-09	Moderate	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-4, AC-9, AU-12, CA-7, CM-3, CM-6, CM-10, CM-11, SC-34, SC-35, SI-4, SI-7
SP 800-82 Rev 3: AU-1, MP-2, SI-3, SI-4, SI-7

SUPPORT RESOURCES

Ensure Your OS Antivirus and Anti-Malware Protections are Active
Control System Defense: Know the Opponent

4.B– IDENTIFY ADVERSE EVENTS

OUTCOME

Organizations can identify adverse security events.

RISK ADDRESSED

Initial access, privilege escalation, and lateral movement.

SCOPE

Organization-wide.

RECOMMENDED ACTION

Ensure the organization has defined clear criteria and processes for adverse events. If an adverse event is suspected, follow the protocol outlined in the incident response plan to escalate the situation.

Automate event information analysis as much as possible to accelerate the investigative timeline for managing suspected adverse events. This will give analysts the time and capacity to mitigate these events effectively.

Conduct analyst role-specific training on the proper protocols and procedures to follow in the event of a suspected cyber incident.

OT: Organizations should account for OT-specific events and anomalies in their processes and environments. It's important to recognize that certain tools and alerts for behaviors or events that could indicate an intrusion might actually be normal within the OT environment.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
DE.AE-08	Moderate	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: IR-4, IR-8
SP 800-82 Rev 3: IR-4

SUPPORT RESOURCES

Planning Considerations for Cyber Incidents
Cybersecurity Incident & Vulnerability Response Playbooks
Continuously Hunt for Network Intrusions

5.A ESTABLISH INCIDENT COMMUNICATION PROCEDURES

OUTCOME

Coordinate crisis communication methods between internal and external organization partners and critical suppliers.

RISK ADDRESSED

Without established communication procedures, incidents can disrupt coordination among response teams, slowing incident resolution, increasing downtime, and amplifying overall damage.

SCOPE

Organization-wide.

RECOMMENDED ACTION

Design a communications plan that identifies stakeholders and mechanisms for coordination and communications during an incident.

Collaborate with stakeholders and securely share information consistent with response plans and information-sharing agreements. Priorities for sharing information include preventing the spread of infections to other systems and networks.

Regularly update senior leadership on the status of major incidents.

Notify human resources when malicious insider activity occurs.

Establish and follow media communications procedures for incident response that comply with the organization's policies on media interaction and information disclosure.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
RS.CO-03	Low	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: IR-4, IR-6, IR-7, SR-3, SR-8
SP 800-82 Rev 3: IR-4, IR-6

SUPPORT RESOURCES

Guidance on effective communications in a cyber incident
Incident Management

5.B ESTABLISH INCIDENT REPORTING PROCEDURES

OUTCOME

CISA and other organizations are better able to provide assistance or understand the broader scope of a cyber incident.

RISK ADDRESSED

Without timely incident reporting, CISA and other groups are less able to assist affected organizations and lack critical insight into the broader threat landscape, such as whether a broader attack is occurring against a specific sector.

SCOPE

Organization-wide.

RECOMMENDED ACTION

Organizations maintain policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or sector risk management agencies [SRMAs] as required, information sharing and analysis centers [ISACs], information sharing and analysis organizations [ISAOs], and CISA).

Known incidents are reported to CISA as well as other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely feasible.

NIST CSF 2.0 REFERENCE(S)	COST	IMPACT	EASE OF IMPLEMENTATION
RS.CO-02, RS.MA-01	Moderate	High	Moderate

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: IR-4, IR-6, IR-7, IR-8, SR-3, SR-8
SP 800-82 Rev 3: IR-4, IR-6, IR-8

SUPPORT RESOURCES

Cybersecurity Incident Response
Critical Infrastructure Threat Information Sharing Framework
Cyber Incident Reporting

6.A– EXECUTE INCIDENT RECOVERY PLAN

OUTCOME

Organizations are capable of safely and effectively recovering from a cybersecurity incident.

RISK ADDRESSED

Disruption to the availability of an asset, service, or system.

SCOPE

Organizational assets.

RECOMMENDED ACTION

Execute plans to recover and restore service to business- or mission-critical assets or systems that might be impacted by a cybersecurity incident. This may include the ability to execute mission essential functions in a degraded manner without access to critical assets or even internet access (e.g., shift to paper-based operations, radio communications, etc.)

Complete post-incident analysis to identify areas for improvement and refine the incident response plan. Focus on incorporating lessons learned, enhancing detection and response capabilities, updating policies and procedures including training, and ensuring that all stakeholders are informed of the changes.

NIST CSF 2.0 REFERENCE(S)

RC.RP-01, ID.IM-02, ID.IM-04

COST	IMPACT	EASE OF IMPLEMENTATION
Moderate	High	Complex

ADDITIONAL NIST REFERENCES

SP 800-53 Rev 5: AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, CP-2, CP-10, IA-1, IR-1, IR-4, IR-8, MA-1, MP-1, PE-1, PL-1, PM-1, PS-1, PT-1, RA-1, SA-1, SC-1, SI-1, SR-1, CA-2, CA-5, CA-7, CA-8, CP-2, CP-4, IR-3, IR-4, IR-8, PL-2, PM-4, PM-31, RA-3, RA-5, RA-7, SA-8, SA-11, SI-2, SI-4, SR-2, SR-5
SP 800-82 Rev 3: CA-2, CA-5, CP-4, CP-1, CP-2, CP-10, IR-1,IR-8, RA-3, SA-11, SR-6

SUPPORT RESOURCES

Incident Response Training
Cybersecurity Incident & Vulnerability Response Playbook
Incident Response Plan (IRP) Basics

GLOSSARY

Access Control Lists: A mechanism that implements access control for a system resource by enumerating the identities of the system entities that are permitted to access the resources. From: NIST SP 800-82 Rev. 3

Administrative Domain: A logical collection of hosts and network resources (e.g., department, building, company, organization) governed by common policies. From: NISTIR 4735

Assets: A person, structure, facility, information, material, or process that has value. From: DHS Risk Lexicon

Automatic Account Lockout or Account Lockout Threshold: Policy that determines the number of failed sign-in attempts that will cause a user account to be locked. From: Account lockout threshold

Baseline Configuration: A documented set of specifications for an information system, or a configuration item within a system, which has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. From: CNSSI 4009-2015

Business Impact Assessment or Business Impact Analysis: An analysis of an information system's requirements, functions, and interdependencies used to characterize system contingency requirements and priorities in the event of a significant disruption. From: NIST SP 800-34 Rev. 1

Change Management: The practice of applying a structured approach to transition an organization from a current state to a future state to achieve expected benefits.

Configuration: The possible conditions, parameters, and specifications with which an information system or system component can be described or arranged. From: NIST SP 800-128

Continuous Monitoring: Maintaining ongoing awareness to support organizational risk decisions. From: NIST SP 800-137

Common Vulnerabilities and Exposures (CVEs): A nomenclature and dictionary of security-related software flaws. From: NIST SP 800-126 Rev. 3

Compensating Controls: The security and privacy controls implemented in lieu of the controls in the baselines described in NIST Special Publication 800-53 that provide equivalent or comparable protection for a system or organization. From: NIST SP 800-37 Rev. 2

Control Systems: A system in which deliberate guidance or manipulation is used to achieve a prescribed value for a variable. Control systems include supervisory control and data acquisition (SCADA), distributed control systems (DCS), programmable logic controllers (PLCs), and other types of industrial measurement and control systems. From: NIST SP 800-82 Rev. 3

Cybersecurity Awareness Training or IT Security Awareness and Training Program: Explains proper rules of behavior for the use of agency information systems and information. The program communicates information technology (IT) security policies and procedures that need to be followed.

Cybersecurity Response Plans or Incident Response Plan: The documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious actions against an organization's information systems(s). From: NIST SP 800-34 Rev. 1

Default Passwords: Factory default software configurations for embedded systems, devices, and appliances often include simple, publicly documented passwords. These systems usually do not provide a full operating system interface for user management, and the default passwords are typically identical (shared) among all systems from a vendor or within product lines. Default passwords are intended for initial testing, installation, and configuration operations, and many vendors recommend changing the default password before deploying the system in a production environment. From: CISA Alert TA13-175A

Demilitarized Zone (DMZ): A perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from intrusions. From: NIST SP 1800-12

Encrypt: Cryptographically transform data to produce cipher text. From: IETF RFC 4949 Ver2

Encryption: Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data. From: NIST SP 800-101 Rev. 1

Executable Files or Executable: Perform indicated tasks according to encoded instructions—commonly used in reference to a computer program or routine.

Firewall: An inter-network connection device that restricts data communication traffic between two connected networks. A firewall may be either an application installed on a general-purpose computer or a dedicated platform (appliance) that forwards or rejects/drops packets on a network. Typically, firewalls are used to define zone borders. Firewalls generally have rules restricting which ports are open. From: NIST SP 800-82 Rev. 3

Firmware: Software program or set of instructions programmed on the flash read-only memory (ROM) of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware. From: NISTIR 8183

Hashing: A process of applying a mathematical algorithm against a set of data to produce a numeric value (a "hash value") that represents the data. From: NIST SP 800-72

Human-Machine Interface (HMI): Software and hardware that allows human operators to monitor the state of a process under control, modify control settings to change the control objective, and manually override automatic control operations in the event of an emergency. The HMI also allows a control engineer or operator to configure set points or control algorithms and parameters in the controller. The HMI also displays process status information, historical information, reports, and other information to operators, administrators, managers, business partners, and other authorized users. Operators and engineers use HMIs to monitor and configure set points, control algorithms, send commands, and adjust and establish parameters in the controller. The HMI also displays process status information and historical information. From: NIST SP 800-82 Rev. 2

Incident Response Plan: A set of predetermined and documented procedures to detect and respond to a cyber incident. From: NIST SP 800-34 Rev. 1

Information Sharing and Analysis Organizations (ISAOs): Any formal or informal entity or collaboration created or employed by public or private sector organizations for the purposes of: a) Gathering and analyzing critical infrastructure information in order to better understand security problems and interdependencies related to critical infrastructure and protected systems, so as to ensure the availability, integrity, and reliability thereof; b) Communicating or disclosing critical infrastructure information to help prevent, detect, mitigate, or recover from the effects of a interference, compromise, or incapacitation problem related to critical infrastructure or protected systems; and c) Voluntarily disseminating critical infrastructure information to its members, as well as state, local, and federal governments; or any other entities that may be of assistance in carrying out the purposes specified above. From: Homeland Security Act of 2002, 6 U.S.C. § 650(13)

Information Sharing and Analysis Centers (ISACs): Trusted entities established by critical infrastructure owners and operators to foster information sharing and best practices about physical and cyber threats and mitigation. From: "National Council of ISACs: About Isacs." Accessed August 20, 2025. From: https://www.nationalisacs.org/about-isacs

Information Technology (IT): Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. From: NIST SP 800-12 Rev. 1

International Electrotechnical Commission (IEC): The IEC is a global, not-for-profit membership organization that brings together 173 countries and coordinates the work of 20,000 experts globally. IEC International Standards and Conformity assessment work underpins international trade in electrical and electronic goods. It facilitates electricity access, and verifies the safety, performance, and interoperability of electrical and electronic devices and systems, including for example consumer devices such as mobile phones or refrigerators, office and medical equipment, information technology, and electricity generation. From: https://www.iec.ch/homepage

International Society of Automation (ISA): A non-profit professional association founded in 1945 to create a better world through automation. ISA advances technical competence by connecting the automation community to achieve operational excellence and is the trusted provider of standards-based foundational technical resources, driving the advancement of individual careers and the overall profession. ISA develops widely used global standards; certifies professionals; provides education and training; publishes books and technical articles; hosts conferences and exhibits; and provides networking and career development programs for its members and customers around the world. From: "International Society of Automation" https://www.isa.org/

International Society of Automation/International Electrotechnical Commission (ISA/IEC) 62443: The ISA/IEC 62443 series of standards, developed by the ISA99 committee and adopted by the International Electrotechnical Commission (IEC), provides a flexible framework to address and mitigate current and future security vulnerabilities in industrial automation and control systems (IACSs). From: See ISA/IEC entries above.

Inventory: The formal listing or property record of personal property assigned to an organization.

Known Exploitable Vulnerabilities Catalog: A list of vulnerabilities that CISA has identified as being exploited, or that have been used by threat actors. As a part of the Binding Operations Directive 22-01, the catalog instructs Federal Civilian Executive Branch (FCEB) agencies that they must remediate these issues within the specific time frame, in order to protect federal infrastructure and reduce incidents. From: CISA KEV

Least Privilege: The principle that a security architecture is designed so that each entity is granted the minimum system resources and authorizations that the entity needs to perform its function. From: NIST SP 800-53 Rev. 5

Logs: A record of the events occurring within an organization's systems and networks. From: NIST SP 800-92

Microsoft Office Macros: A macro in Access is a tool that automates tasks and adds functionality to forms, reports, and controls. For example, when a command button is added to a form, the button's OnClick event is associated with the macro. From: "Introduction to Access Programming," https://support.microsoft.com/en-us/office/introduction-to-access-programming-92eb616b-3204-4121-9277-70649e33be4f

National Institute of Standards and Technology (NIST): The National Institute of Standards and Technology promotes U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve quality of life. From: NIST

Network Segmentation and Segregation: Network segmentation involves partitioning a network into smaller networks, while network segregation involves developing and enforcing a rule set for controlling the communications between specific hosts and services. From: "Introduction to Access Programming." https://support.microsoft.com/en-us/office/introduction-to-access-programming-92eb616b-3204-4121-9277-70649e33be4f

NIST Cybersecurity Framework (CSF): A set of cybersecurity activities and references that are common across critical infrastructure sectors and are organized around particular outcomes. The Framework Core is composed of four types of elements: functions, categories, subcategories, and informative references. From: NIST CSF

NIST Risk Management Framework: The Risk Management Framework (RMF), presented in NIST SP 800-37, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. From: NIST SP 800-37 Rev. 2: RMF

NIST SP 800-30: Provides guidance for conducting risk assessments of federal information systems and organizations, amplifying the guidance in Special Publication 800-39. Risk assessments, carried out at all three tiers in the risk management hierarchy, are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. From: NIST SP 800-30

NIST SP 800-53: This publication establishes controls for systems and organizations. The controls can be implemented within any organization or system that processes, stores, or transmits information. The use of these controls is mandatory for federal information systems. NIST SP 800-53 accomplishes this objective by providing a comprehensive and flexible catalog of security and privacy controls to meet current and future protection needs based on changing threats, vulnerabilities, requirements, and technologies. The publication also improves communication among organizations by providing a common lexicon that supports the discussion of security, privacy, and risk management concepts. From: NIST SP 800-53 Rev. 5

NIST SP 800-82: Provides guidance for securing industrial control systems (ICS), including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other systems performing control functions. The document provides a notional overview of ICS, reviews typical system topologies and architectures, identifies known threats and vulnerabilities to these systems, and provides recommended security countermeasures to mitigate the associated risks. From: NIST 800-82 Rev. 3

Operational Technology (OT): Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems/devices detect or cause a direct change through the monitoring and/or control of devices, processes, and events. Examples include ICSs, building management systems, fire control systems, and physical access control mechanisms.

Penetration Testing (Remote): Simulates the tactics and techniques of real-world threat actors to identify and validate exploitable pathways. This service is ideal for testing perimeter defenses, the security of externally available applications, and the potential for exploitation of open-source information. From: NIST SP 800-37 Rev. 2

Phishing: A digital form of social engineering to deceive individuals into providing sensitive information.

Phishing-Resistant MFA: As defined in Office of Management and Budget Memorandum 22-09, authentication processes designed to detect and prevent disclosure of authentication secrets and outputs to a website or application masquerading as a legitimate system. From: OMB M-22-09

Privileged Accounts: An information system account with approved authorizations of a privileged user. From: CNSSI 4009-2015

Remote Desktop Protocol (RDP): Microsoft proprietary protocol that enables remote connections to other computers, typically over TCP port 3389. It provides network access for a remote user over an encrypted channel. Network administrators use RDP to diagnose issues, log in to servers, and to perform other remote actions. Remote users use RDP to log in to the organization's network to access email and files. From: "MS-ISAC Security Primer - Remote Desktop Protocol" https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol

Salting Passwords or Password Salt: A random number added to a password to make it more difficult to crack. It is common practice to take passwords and run them through a hashing algorithm and store the results in the login database. When users enter their passwords, they are once again hashed and matched against the database. A salt is a random number added to the password prior to hashing to make the result more difficult to uncover by using a "brute force" dictionary attack. From: "MS-ISAC Security Primer - Remote Desktop Protocol" https://www.cisecurity.org/insights/white-papers/security-primer-remote-desktop-protocol

System Architecture: An architecture is the fundamental organization of a system, embodied in its components, their relationships with each other and the environment, and the principles governing its design and evolution. From: "ISO/IEC/IEEE 42010:2022." https://www.iso.org/standard/74393.html

Table-Top Exercise (TTX): A discussion-based exercise where personnel with roles and responsibilities in a particular IT plan meet in a classroom setting or in breakout groups to validate the content of the plan by discussing their roles during an emergency and their responses to a particular emergency situation. A facilitator initiates the discussion by presenting a scenario and asking questions based on the scenario. From: NIST SP 800-84

Transport Layer Security (TLS): An authentication and encryption protocol widely implemented in browsers and web servers. HTTP traffic transmitted using TLS is known as HTTPS. From: NISTIR 7711

Vulnerability Disclosure Program: Gives security researchers clear guidelines for conducting vulnerability discovery activities and conveys CISA preferences for submitting discovered vulnerabilities to an organization. From: CISA Vulnerability Disclosure Policy

ACKNOWLEDGMENTS

The cybersecurity performance goals would not have been possible without crosscutting input from public and private stakeholders. CISA and NIST would like to thank the following companies, organizations, U.S. federal agencies, and international partners for their contributing comments on these goals:

1898 & Co; AAC Cyber Group; ABS Group; Administration for Strategic Preparedness and Response (ASPR); Amazon Web Services; American Chemistry Council (AAC) Cybersecurity Information Sharing Group; American Fuel and Petrochemical Manufacturers (AFPM); American Gas Association; American Petroleum Institute (API); American Public Power Association (APPA); American Water Works Association; Area Maritime Security Committee Houston-Galveston; Bechtel; Boeing; Chemical Sector Coordinating Council (CSCC); City of Crystal, Minnesota; City of Phoenix Department of Aviation (Phoenix Sky Harbor International Airport); City of Pittsburgh Housing Authority; Claroty; Colorado River Energy Distributors Association; Consolidated Communications; CTIA, NCTA, USTelecom; Cyber Risk Institute; Cyber Threat Alliance; D.L.; Discover Financial Services; Eclypsium, Inc.; Dragos; Edison Electric Institute; Enbridge, Inc.; Exxon; Federal Deposit Insurance Corporation (FDIC); Federal Housing Finance Agency (FHFA); Federal Reserve (and Federal Reserve, Financial Services); FERC, Division of Dam Safety and Inspections; Financial Services Sector Coordinating Council (FSSCC); FireEye; GE; Granite Falls Consulting; Information Security Officer, Maersk Line, Limited; Honeywell; Information Technology Industry Council (ITI); Israel National Cyber Directorate (INCD); IT Sector Coordinating Council (IT-SCC); JP Morgan; Marsh; Matson Navigation Company; Microsoft; National Air Transportation Association; National Rural Electric Cooperative Association (NRECA); National Water Resources Association (CREDA/NWRA); National Cyber Security Centre (NCSC (UK)); NCTA; Netrise; Network Perception; Netwrix Corporation; Nozomi Networks; NTCA – The Rural Broadband Association; Office of the Comptroller of the Currency (OCC); Operational Technology Cybersecurity Coalition; Port Authority of New York and New Jersey; Port of Houston Authority; Schneider Electric; Securities and Exchange Commission (SEC); Securities Investor Protection Corporation (SIPC); Sera-Brynn Consulting; Siemens Government Technologies; Southern California Edison; Southern Company; State of Washington, Cybersecurity & Critical Infrastructure Protection Unit; Transportation Security Administration (TSA); U.S. Army, Materiel Command; U.S. Department of Energy (DOE); U.S. Environmental Protection Agency (EPA); U.S. Nuclear Regulatory Commission; U.S. Coast Guard; University of Miami Health System; U.S. Mint – Philadelphia; Both public and private members of CISA's Control Systems Working Group (CSWG) and Control Systems Interagency Working Group (CSIWG); Department of Health and Human Services (HHS), Food and Drug Administration (FDA), Office of the National Coordinator for Health Information Technology (ONC); Water Environment Federation; Water Sector Coordinating Council; Waterfall Security; Woodard & Curran; Xylem.

In addition to organizations, CISA would like to recognize the following individuals who provided particularly valuable feedback:

Marco Ayala, David Batz, Bryson Bort, Mark Bristow, Lance Cleghorn, Josh Corman, Curt Dukes, Danielle Jablanksi, Chris Jager, Isaiah Jones, Robert M. Lee, Joe Marshall, Patrick Miller, Thomas Reagan, Alexander Romero, Marty Rubin, Kimberly Sanders, Gus Serino, and Nicole Thompson.