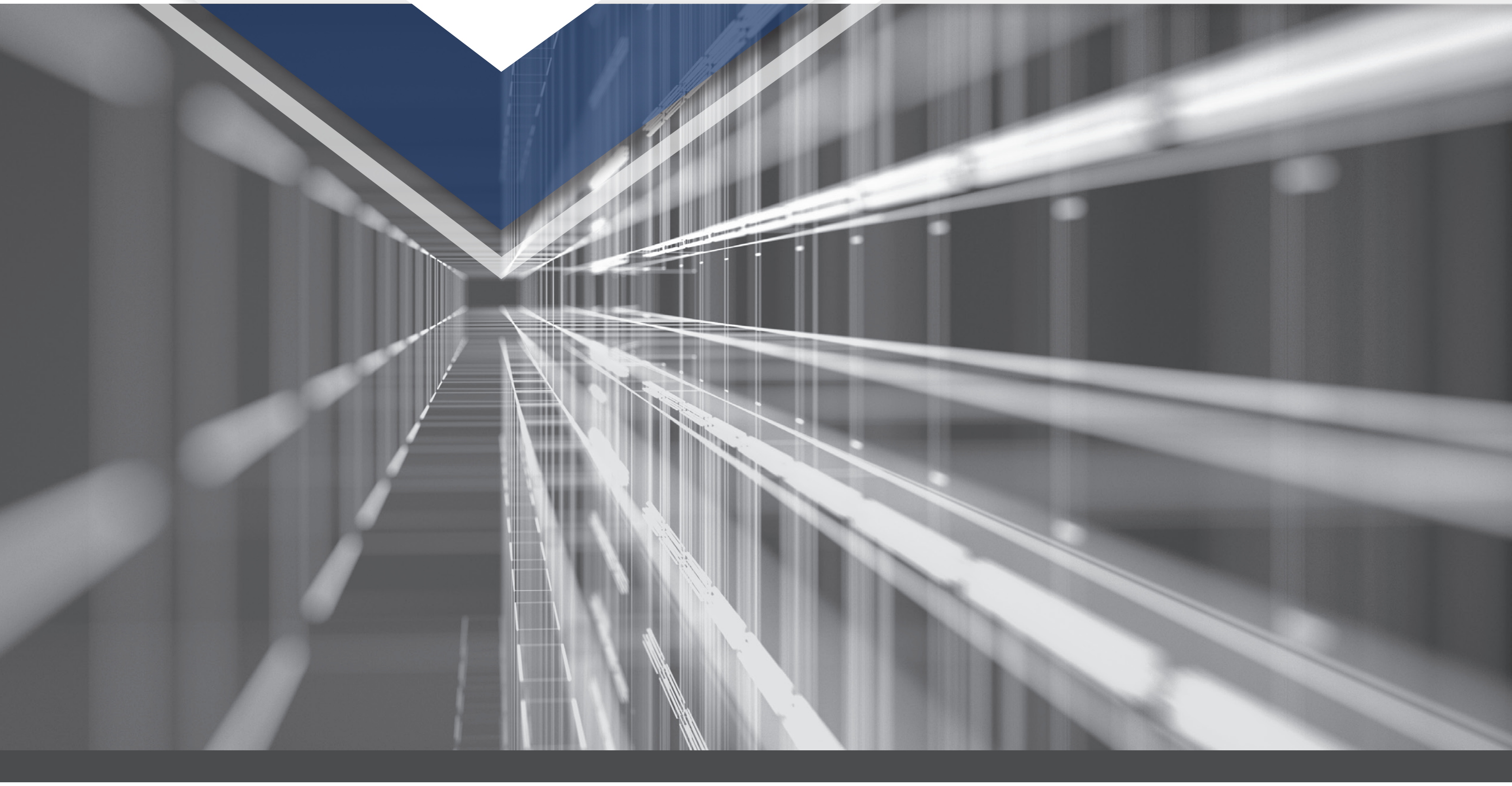
CPG

Cross-Sector Cybersecurity
Performance Goals

March 2023 Update



PERFORMANCE GOALS

Version: 1.0.1

A LETTER FROM OUR DIRECTOR

As the nation's cyber defense agency, one of CISA's most important roles is to understand the challenges facing organizations, both large and small, in order to make progress on the shared goal of reducing cyber risk to the critical infrastructure Americans rely on every day. Over the past several years, as our nation has faced unprecedented cyber threats from ransomware to nation-state espionage, we have heard a common refrain from organizations across the spectrum, from the largest multinational corporations to state and local governments, to critical infrastructure entities of all sizes: How can we focus investment toward the most impactful security outcomes?

We hear small- and medium-sized hospitals and utilities ask how they can make progress with limited budgets, staffing, and expertise. We hear organizations with mature cyber programs ask what more they can do to prevent attacks from advanced threat actors, manage risks to less mature organizations in their supply chain, and help reduce broader risk to the nation. We hear the global Operational Technology and Industrial Control Systems (OT/ICS) community clamor to be seen and recognized alongside traditional IT security and supported in their essential role of defending our increasingly connected electric grids, hospitals, water facilities, and other critical infrastructure.

It became clear that even with comprehensive guidance from sources like the NIST Cybersecurity Framework, many organizations would benefit from help identifying and prioritizing the most important cybersecurity practices along with support in making a compelling argument to ensure adequate resources for driving down risk. Ultimately, prioritized investment will help meaningfully address serious risks to the safety, health, and livelihoods of the American people.

The Cross-Sector Cybersecurity Performance Goals (CPGs) strive to address this need by providing an approachable common set of IT and OT cybersecurity protections that are clearly defined, straightforward to implement, and aimed at addressing some of the most common and impactful cyber risks. The CPGs are written and designed to be easy to understand and relatively easy to communicate with non-technical audiences, including senior business leadership.

Informed by extensive input from experts across sectors, public and private, domestic and international, the CPGs reflect some of the best thinking gleaned from across the cybersecurity community. As in all things, we look forward to continuous feedback on them so we can regularly refresh these goals based on the constantly evolving technology and threat landscapes. Ultimately, our hope is that the CPGs will not only serve as a strong foundation for improving cybersecurity across our nation's critical infrastructure sectors, but also as a baseline of security outcomes that merit the trust of the American people.

JEN
Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency (CISA)
October 2022

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. By leveraging partnerships across all critical infrastructure sectors and working with their respective sector risk management agencies (SRMAs), gathering insights from government partners both in the U.S. and abroad, and conducting our own cyber assessments, hunts, and incident response efforts, CISA regularly observes patterns across our critical infrastructure where essential cybersecurity best practices are not sufficiently applied. Subject matter experts and critical infrastructure operators providing input during the course of this document's development shared similar observations.

Our concerns with these gaps are more than hypothetical. Our nation has seen the real impact of some of these gaps, whether ransomware attacks that affect critical functions from hospitals to school districts or 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.

Over the past year, CISA has worked with hundreds of partners, received thousands of comments, and analyzed years of data from our efforts to assess, protect, and respond to cyber incidents. This has enabled us to identify key challenges that leave our nation at serious risk.

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

2. **Small- and medium-sized organizations are left behind**. Organizations with limited resources or less mature cybersecurity programs often face challenges determining where to start to put in place reasonable cybersecurity measures. While existing resources like the NIST Cybersecurity Framework are invaluable, small organizations face difficulties in identifying where to invest for the greatest impact to their cybersecurity posture and specific guidance on how to effectively implement cybersecurity protections.

3. **Lack of consistent standards and cyber maturity across critical infrastructure sectors**. There is significant inconsistency in cybersecurity capabilities, investment, and baseline practices within and across critical infrastructure sectors. This inconsistency leads to gaps that can be exploited by threat actors to cause functional and cascading impacts.

4. **OT cybersecurity often remains overlooked and under-resourced**. The cybersecurity industry is still largely focused on business IT systems, often neglecting the critical risk in OT systems, which were designed to optimize reliability and availability and often lack native security capabilities. This puts critical infrastructure entities at serious risk as more OT devices become network-connected. Even so, many critical infrastructure entities lack adequate OT cybersecurity programs, especially where cybersecurity is still seen as primarily an IT concern. Entities that do have OT cybersecurity programs often lack basic OT cyber protections and are unable to find relevant OT-specific guidance for their environments.

CONTENT

CONFRONTING THIS CHALLENGE: National Security Memorandum 5

In July 2021, President Biden signed National Security Memorandum (NSM)-5: Improving Cybersecurity for Critical Infrastructure Control Systems. This memorandum required CISA, in coordination with the National Institute of Standards and Technology (NIST) and the interagency community, to develop baseline cybersecurity goals that are consistent across all critical infrastructure sectors. This document contains the latest iteration of the Cross-Sector Cybersecurity Performance Goals (CPGs). Additionally, in late 2022, CISA began working with Sector Risk Management Agencies (SRMAs) to build on this foundation to develop sector-specific goals.

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 and are informed by the most common and impactful threats and adversary tactics, techniques, and procedures (TTPs) observed by CISA and its government and industry partners, making 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 and aim to help critical infrastructure entities, particularly small and medium organizations, get started on their path toward a strong cybersecurity posture. As such, the CPGs are intended to be a floor, not a ceiling, for what 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 risks 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, and will be followed by sector-specific goals that dive deeper into the unique constraints, threats, and maturity of each sector where applicable.
- **A risk management or full cybersecurity program:** The CPGs do not cover broader approaches to risk management or risk prioritization, which are well articulated in other frameworks such as the NIST Cybersecurity Framework (NIST CSF).
- **Mandated by CISA:** The CPGs are intended to be voluntarily adopted by organizations 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.)

The CPGs will be regularly updated, with a targeted revision cycle of at least every 6 to 12 months. CISA has set up a Discussions page to receive feedback and ideas for new CPGs. A link to this site will also be available via https://www.cisa.gov/cpgs.

CPG SELECTION CRITERIA

As previously mentioned, the CPGs are a subset of cybersecurity practices, selected through a thorough 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 even 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 (ZT)" would not be a suitable CPG, as this practice is vague, insufficiently defined, hard to measure, and can be overly burdensome for small organizations.

CPG MODEL

The CPGs in this document are displayed 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, what "good" looks like, and other important information.

Each goal is comprised of the following components:

MODEL COMPONENT	COMPONENT DESCRIPTION
Outcome	The ultimate security outcome that each CPG strives to enable.
TTP/Risk Addressed	Either (a) the primary set of MITRE ATT&CK TTPs or (b) the set of organizational risks that would be rendered less likely or impactful if the goal is implemented.
Security Practice	The mitigation(s) that organizations should implement to achieve the outcome and reduce the impact of the TTP or risk.
Scope	The set or subset of assets to which organizations should apply the security practice.
Recommended Action	Example approaches to help organizations progress toward achievement of the performance goal, based on input from CISA's collaborative stakeholder process. These actions will be updated regularly as new threats and defenses are identified.
NIST CSF Reference	The CSF subcategory that most closely relates to the security practice.

HOW ARE THESE DIFFERENT FROM NIST CSF AND OTHER STANDARDS?

Plenty of existing cybersecurity guidance and frameworks exist — 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 adoption of the NIST CSF by every organization to enable development and maintenance of a sustainable, risk information cybersecurity program. Based on stakeholder feedback, the CPGs can be leveraged by organizations 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 Getting 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 is mapped 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 Package Contents

There are three documents provided on the CPGs:

1. The CPG List (this document).
2. The CPG Worksheet (attached PDF). See more below.
3. The CPG Full Data Matrix (attached Excel document), which contains all the raw data of the CPGs, their mappings to other frameworks, and more.

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.

The worksheet includes general estimates of the cost, complexity, and impact of implementing each goal. These estimates are intended to be used 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 are already implemented. Organizations may have already implemented some or many of the CPGs through their adherence to existing guidance or regulation, such as NIST CSF or ISA 62443, and all CPGs are mapped to corresponding controls in those common frameworks.
2. Identify and prioritize gaps. Organizations 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 the previous steps. 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

MARCH 2023 UPDATE: How Have the CPGs Changed Since Their Initial Publication?

After CISA published the first CPG report in October 2022, the agency received feedback from multiple sectors asking for more streamlined mapping to the NIST CSF. In response, CISA has reorganized the CPGs to align to NIST CSF functions (Identify, Protect, Detect, Respond, and Recover). Note that several goals map to multiple functions, and implementation of a given CPG does not necessarily constitute complete fulfillment of the referenced NIST CSF subcategory.

- This March 2023 update, version 1.0.1, reorders and renumbers the CPGs to align closely with NIST CSF functions. Accompanying documents (the Checklist and Matrix) have been adjusted accordingly. Mappings from the original numbering are reflected in the Matrix for users who may be familiar with the original publication.
- Additionally, the MFA goal has been updated to reflect the most recently published CISA guidance regarding phishing-resistant MFA and the considerations for prioritizing implementation.
- CISA has also added a goal based on GitHub feedback to aid in organizations' recovery planning.
- Finally, slight modifications have been made to the glossary to reflect the minor content changes listed above, as well as to the acknowledgment section to thank additional stakeholders who contributed to the current and previous version.

IDENTIFY

1.A ASSET INVENTORY

ID.AM-1, ID.AM-2, ID.AM-4, DE.CM-1, DE.CM-7

OUTCOME

Better identify known, unknown (shadow), and unmanaged assets, and more rapidly detect and respond to new vulnerabilities.

TTP or RISK ADDRESSED

- Hardware Additions (T1200)
- Exploit Public-Facing Application (T0819, ICS T0819)
- Internet Accessible Device (ICS T0883)

SCOPE

IT and OT assets

RECOMMENDED ACTION

Maintain a regularly updated inventory of all organizational assets with an IP address (including IPv6), including OT. This inventory is updated on a recurring basis, no less than monthly for both IT and OT.

1.B ORGANIZATIONAL CYBERSECURITY LEADERSHIP

ID.GV-1, ID.GV-2

OUTCOME

A single leader is responsible and accountable for cybersecurity within an organization.

TTP or RISK ADDRESSED

Lack of sufficient cybersecurity accountability, investment, or effectiveness.

SCOPE

N/A

RECOMMENDED ACTION

A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of cybersecurity activities. This role may undertake activities such as managing cybersecurity operations at the senior level, requesting and securing budget resources, or leading strategy development to inform future positioning.

1.C OT CYBERSECURITY LEADERSHIP

ID.GV-1, ID.GV-2

OUTCOME

A single leader is responsible and accountable for OT-specific cybersecurity within an organization with OT assets.

TTP or RISK ADDRESSED

Lack of accountability, investment, or effectivness of OT cybersecurity program.

SCOPE

N/A

RECOMMENDED ACTION

A named role/position/title is identified as responsible and accountable for planning, resourcing, and execution of OT-specific cybersecurity activities. In some organizations, this may be the same position as identified in 1.B.

1.D IMPROVING IT AND OT CYBERSECURITY RELATIONSHIPS

ID.GV-2, PR.AT-5

OUTCOME

Improve OT cybersecurity and more rapidly and effectively respond to OT cyber incidents.

TTP or RISK ADDRESSED

Poor working relationships and a lack of mutual understanding between IT and OT cybersecurity can often result in increased risk for OT cybersecurity.

SCOPE

All IT and OT security personnel

RECOMMENDED ACTION

Organizations sponsor at least one “pizza party” or equivalent social gathering per year that is focused on strengthening working relationships between IT and OT security personnel and is not a working event (such as providing meals during an incident response).

1.E MITIGATING KNOWN VULNERABILITIES

ID.RA-1, PR.IP-12, DE.CM-8, RS.MI-3, ID.RA-6, RS.AN-5

OUTCOME

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

TTP or RISK ADDRESSED

- Active Scanning - Vulnerability Scanning (T1595.002)
- Exploit Public-Facing Application (T1190, ICS T0819)
- Exploitation of Remote Service (T1210, ICS T0866)
- Supply Chain Compromise (T1195, ICS T0862)
- External Remote Services (T1133, ICS T0822)

SCOPE

Internet-facing assets

RECOMMENDED ACTION

All known exploited vulnerabilities (listed in CISA's Known Exploited Vulnerabilities Catalog in internet-facing systems are patched or otherwise mitigated within a risk-informed span of time, prioritizing more critical assets first.

OT: For 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.

1.F THIRD-PARTY VALIDATION OF CYBERSECURITY CONTROL EFFECTIVENESS

ID.RA-1, ID.RA-3, ID.RA-4, ID.RA-5, ID.RA-6

OUTCOME

Identify TTPs that lack proper defenses and establish confidence in organizational cyber defenses.

TTP or RISK ADDRESSED

Reduce risk of gaps in cyber defenses or a false sense of security in existing protections.

SCOPE

IT and OT assets and networks

RECOMMENDED ACTION

Third parties with demonstrated expertise in (IT and/or OT) cybersecurity regularly validate the effectiveness and coverage of an organization's cybersecurity defenses. These exercises, which may include penetration tests, bug bounties, incident simulations, or table-top exercises, should include both unannounced and announced tests.

Exercises consider both the ability and impact of a potential adversary to infiltrate the network from the outside, as well as the ability of an adversary within the network (e.g., "assume breach") to pivot laterally to demonstrate potential impact on critical systems, including operational technology and industrial control systems.

High-impact findings from previous tests are mitigated in a timely manner and are not re-observed in future tests.

1.G SUPPLY CHAIN INCIDENT REPORTING

ID.SC-1, ID.SC-3

OUTCOME

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

TTP or RISK ADDRESSED

Supply Chain Compromise (T1195, ICS T0862)

SCOPE

Suppliers of IT and OT assets and services

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 within a risk-informed time frame as determined by the organization.

1.H SUPPLY CHAIN VULNERABILITY DISCLOSURE

ID.SC-1, ID.SC-3

OUTCOME

Organizations more rapidly learn about and respond to vulnerabilities in assets provided by vendors and service providers.

TTP or RISK ADDRESSED

Supply Chain Compromise (T1195, ICS T0862)

SCOPE

Suppliers of IT and OT assets and services

RECOMMENDED ACTION

Procurement documents and contracts, such as SLAs, stipulate that vendors and/or service providers notify the procuring customer of confirmed security vulnerabilities in their assets within a risk-informed time frame as determined by the organization.

1.I

VENDOR/SUPPLIER CYBERSECURITY REQUIREMENTS

ID.SC-3

OUTCOME

Reduce risk by buying more secure products and services from more secure suppliers.

TTP or RISK ADDRESSED

Supply Chain Compromise (T1195, ICS T0862)

SCOPE

Suppliers of IT and OT assets and services

RECOMMENDED ACTION

Organizations' procurement documents include cybersecurity requirements and questions, which are evaluated in vendor selection such that, given two offerings of roughly similar cost and function, the more secure offering and/or supplier is preferred.

PROTECT

2.A– CHANGING DEFAULT PASSWORDS — PR.AC-1

OUTCOME

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

TTP or RISK ADDRESSED

- Valid Accounts - Default Accounts (T1078.001)
- Valid Accounts (ICS T0859)

SCOPE

Password-protected IT assets and newly acquired OT assets.

RECOMMENDED ACTION

An enforced organization-wide policy and/or process that requires changing default manufacturer passwords for any/all hardware, software, and firmware before putting on any internal or external network. This includes IT assets for OT, such as OT administration web pages.

In instances where changing default passwords is not feasible (e.g., a control system with a hard-coded password), implement and document appropriate compensating security controls, and monitor logs for network traffic and login attempts on those devices.

OT: While changing default passwords on an organization's existing OT requires significantly more work, we still recommend having such a policy to change default credentials for all new or future devices. This is not only easier to achieve, but also reduces potential risk in the future if adversary TTPs change.

2.B– MINIMUM PASSWORD STRENGTH — PR.AC-1

OUTCOME

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

TTP or RISK ADDRESSED

- Brute Force - Password Guessing (T1110.001)
- Brute Force - Password Cracking (T1110.002)
- Brute Force - Password Spraying (T1110.003)
- Brute Force - Credential Stuffing (T1110.004)

SCOPE

Password-protected IT and Windows-based OT assets

RECOMMENDED ACTION

Organizations have a system-enforced policy that requires a minimum password length of 15* or more characters for all password-protected IT assets and all OT assets, 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 length are prioritized for upgrade or replacement.

This goal is particularly important for organizations that lack widespread implementation of MFA and capabilities to protect against brute-force attacks (such as web application firewalls and third-party content delivery networks) or are unable to adopt passwordless authentication methods.

* Modern attacker tools can crack eight-character passwords quickly. Length is a more impactful and important factor in password strength than complexity or frequent password rotations. Long passwords are also easier for users to create and remember.

** OT assets that use a central authentication mechanism (such as Active Directory) are most important to address. Examples of low-risk OT assets that may not be technically feasible include those in remote locations, such as those on offshore rigs or wind turbines.

2.C– UNIQUE CREDENTIALS — PR.AC-1

OUTCOME

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

TTP or RISK ADDRESSED

- Valid Accounts (T1078, ICS T0859)
- Brute Force - Password Guessing (T1110.001)

SCOPE

IT and OT assets

RECOMMENDED ACTION

Organizations provision unique and separate credentials for similar services and asset access on IT and OT networks. Users do not (or cannot) reuse passwords for accounts, applications, services, etc. Service accounts/machine accounts have passwords that are unique from all member user accounts.

2.D – REVOKING CREDENTIALS FOR DEPARTING EMPLOYEES

PR.AC-1, PR.IP-11

OUTCOME

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

TTP or RISK ADDRESSED

Valid Accounts (T1078, ICS T0859)

SCOPE

Departing/Departed Employees

RECOMMENDED ACTION

A defined and enforced administrative process applied to all departing employees by the day of their departure that (1) revokes and securely returns all physical badges, key cards, tokens, etc., and (2) disables all user accounts and access to organizational resources.

2.E – SEPARATING USER AND PRIVILEGED ACCOUNTS

PR.AC-4

OUTCOME

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

TTP or RISK ADDRESSED

Valid Accounts (T1078, ICS T0859)

SCOPE

IT and OT assets, where safe and technically capable

RECOMMENDED ACTION

No user accounts always have administrator or super-user privileges. Administrators maintain separate user accounts for all actions and activities not associated with the administrator role (e.g., for business email, web browsing). Privileges are reevaluated on a recurring basis to validate continued need for a given set of permissions.

2.F – NETWORK SEGMENTATION

PR.AC-5, PR.PT-4

OUTCOME

Reduce the likelihood of threat actors accessing the OT network after compromising the IT network.

TTP or RISK ADDRESSED

- Network Service Discovery (T1046)
- Trusted Relationship (T1199)
- Network Connection Enumeration (ICS T0840)
- Network Sniffing (T1040, ICS T0842)

SCOPE

IT and OT assets, where safe and technically capable

RECOMMENDED ACTION

All connections to the OT network are denied by default unless explicitly allowed (e.g., by IP address and port) for specific system functionality. Necessary communications paths between the IT and OT networks must pass through an intermediary, such as a properly configured firewall, bastion host, "jump box," or a demilitarized zone, which is closely monitored, captures network logs, and only allows connections from approved assets.

2.G – DETECTION OF UNSUCCESSFUL (AUTOMATED) LOGIN ATTEMPTS

PR.AC-7

OUTCOME

Protect organizations from automated, credential-based attacks.

TTP or RISK ADDRESSED

- Brute Force - Password Guessing (T1110.001)
- Brute Force - Password Cracking (T1110.002)
- Brute Force - Password Spraying (T1110.003)
- Brute Force - Credential Stuffing (T1110.004)

SCOPE

Password-protected IT and OT assets, where safe and technically capable

RECOMMENDED ACTION

All unsuccessful logins are logged and sent to an organization's security team or relevant logging system. Security teams are notified (e.g., by an alert) after a specific number of consecutive, unsuccessful login attempts in a short period (e.g., five failed attempts in two minutes). This alert is logged and stored in the relevant security or ticketing system for retroactive analysis.

For IT assets, a system-enforced policy prevents future logins for the suspicious account. For example, this could be for some minimum time, or until the account is re-enabled by a privileged user. This configuration is enabled when available on an asset. For example, Windows 11 can automatically lock out accounts for 10-minutes after 10 incorrect logins over a 10-minute period.

2.H PHISHING-RESISTANT MULTIFACTOR AUTHENTICATION (MFA) PR.AC-7, PR.AC-1

OUTCOME

Add a critical, additional layer of security to protect assets accounts whose credentials have been compromised.

TTP or RISK ADDRESSED

- Brute Force (T1110)
- Remote Services - Remote Desktop Protocol (T1021.001)
- Remote Services - SSH (T1021.004)
- Valid Accounts (T1078, ICS T0859)
- External Remote Services (ICS T0822)

SCOPE

IT and OT assets with remote access, such as workstations and human-machine interfaces (HMIs), where safe and technically capable

RECOMMENDED ACTION

Organizations implement MFA for access to assets using the strongest available method for that asset (see below for scope). MFA options sorted by strength, high to low, are as follows:

1. Hardware-based, phishing-resistant MFA (e.g., FIDO/WebAuthn or public key infrastructure (PKI) based - see CISA guidance in”Resources”);
2. If such hardware-based MFA is not available, then mobile app-based soft tokens (preferably push notification with number matching) or emerging technology such as FIDO passkeys are used;
3. MFA via short message service (SMS) or voice 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: Within OT environments, MFA is enabled on all accounts and systems that can be accessed remotely, including vendors/maintenance accounts, remotely accessible user and engineering workstations, and remotely accessible HMIs.

2.I BASIC CYBERSECURITY TRAINING PR.AT-1

OUTCOME

Organizational users learn and perform more secure behaviors.

TTP or RISK ADDRESSED

User Training (M1017, ICS M0917)

SCOPE

All employees and contractors

RECOMMENDED ACTION

At least annual trainings for all organizational employees and contractors that cover basic security concepts, such as phishing, business email compromise, basic operational security, password security, etc., as well as foster an internal culture of security and cyber awareness.

New employees receive initial cybersecurity training within 10 days of onboarding and recurring training on at least an annual basis.

2.J OT CYBERSECURITY TRAINING PR.AT-2, PR.AT-3, PR.AT-5

OUTCOME

Personnel responsible for securing OT assets received specialized OT-focused cybersecurity training.

TTP or RISK ADDRESSED

User Training (M1017, ICS M0917)

SCOPE

All personnel responsible for OT security

RECOMMENDED ACTION

In addition to basic cybersecurity training, personnel who maintain or secure OT as part of their regular duties receive OT-specific cybersecurity training on at least an annual basis.

2.K STRONG AND AGILE ENCRYPTION PR.DS-2

OUTCOME

Effective encryption deployed to maintain confidentiality of sensitive data and integrity of IT and OT traffic.

TTP or RISK ADDRESSED

- Adversary-in-the-Middle (T1557)
- Automated Collection (T1119)
- Network Sniffing (T1040, ICS T0842)
- Wireless Compromise (ICS T0860)
- Wireless Sniffing (ICS T0887)

SCOPE

All IT traffic and remote OT assets (those that communicate with external entities)

RECOMMENDED ACTION

Properly configured and up-to-date secure socket layer (SSL) / transport layer security (TLS) is utilized to protect data in transit, when technically feasible. Organizations should also plan to identify any use of outdated or weak encryption, update these to sufficiently strong algorithims, and consider managing implications of post-quantum cryptography.

OT: To minimize the impact to latency and availability, encryption is used when feasible, usually for OT communications connecting with remote/external assets.

2.L

SECURE SENSITIVE DATA — PR.DS-1, PR.DS-5

OUTCOME

Protect sensitive information from unauthorized access.

TTP or RISK ADDRESSED

- Unsecured Credentials (T1552)
- Steal or Forge Kerberos Tickets (T1558)
- OS Credential Dumping (T1003)
- Data from Information Repositories (ICS T0811)
- Theft of Operational Information (T0882)

SCOPE

All passwords, credentials, secrets, and other sensitive or controlled information

RECOMMENDED ACTION

Sensitive data, including credentials, are not stored in plaintext anywhere in the organization and can only be accessed by authenticated and authorized users. Credentials are stored in a secure manner, such as with a credential/password manager or vault, or other privileged account management solution.

2.M

EMAIL SECURITY — PR.DS-5, PR.AC-7

OUTCOME

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

TTP or RISK ADDRESSED

- Phishing (T1566)
- Business Email Compromise

SCOPE

All organizational email infrastructure

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." For further examples and information, see CISA's past guidance for federal agencies.

2.N

DISABLE MACROS BY DEFAULT — PR.IP-1, PR.IP-3

OUTCOME

Reduce the risk from embedded macros and similar executive code, a common and highly effective threat actor TTP.

TTP or RISK ADDRESSED

- Phishing - Spearphishing Attachment (T1566.001)
- User Execution - Malicious FIle (T1204.002)

SCOPE

IT assets

RECOMMENDED ACTION

A system-enforced policy that disables Microsoft Office macros, or similar embedded code, by default on all devices. If macros must be enabled in specific circumstances, there is a policy for authorized users to request that macros are enabled on specific assets.

2.O

DOCUMENT DEVICE CONFIGURATIONS — PR.IP-1

OUTCOME

More efficiently and effectively manage, respond to, and recover from cyberattacks against the organization and maintain service continuity.

TTP or RISK ADDRESSED

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

SCOPE

IT and OT assets

RECOMMENDED ACTION

Organizations maintain accurate documentation describing the baseline and current configuration details of all critical IT and OT assets to facilitate more effective vulnerability management and response and recovery activities. Periodic reviews and updates are performed and tracked on a recurring basis.

2.P DOCUMENT NETWORK TOPOLOGY

PR.IP-1, ID.AM-3

OUTCOME

More efficiently and effectively respond to cyberattacks and maintain service continuity.

TTP or RISK ADDRESSED

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

SCOPE

All IT and OT networks

RECOMMENDED ACTION

Organizations maintain accurate documentation describing updated network topology and relevant information across all IT and OT networks. Periodic reviews and updates should be performed and tracked on a recurring basis.

2.Q HARDWARE AND SOFTWARE APPROVAL PROCESS

PR.IP-3

OUTCOME

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

TTP or RISK ADDRESSED

- Supply Chain Compromise (T1195, ICS T0862)
- Hardware Additions (T1200)
- Browser Extensions (T1176)
- Transient Cyber Asset (ICS T0864)

SCOPE

IT and OT assets

RECOMMENDED ACTION

Implement an administrative policy or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed. Organizations maintain a risk-informed allowlist of approved hardware, firmware, and software that includes specification of approved versions, when technically feasible. For OT assets specifically, these actions should also be aligned with defined change control and testing activities.

2.R SYSTEM BACKUPS

PR.IP-4

OUTCOME

Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.

TTP or RISK ADDRESSED

- Data Destruction (T1485, ICS T0809)
- Data Encrypted for Impact (T1486)
- Disk Wipe (T1561)
- Inhibit System Recovery (T1490)
- Denial of Control (ICS T0813)
- Denial/Loss of View (ICS T0815, T0829)
- Loss of Availability (T0826)
- Loss/Manipulation of Control (T0828, T0831)

SCOPE

IT and OT assets necessary for business operations

RECOMMENDED ACTION

All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year).

Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.

2.S INCIDENT RESPONSE (IR) PLANS

PR.IP-9, PR.IP-10

OUTCOME

Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.

TTP or RISK ADDRESSED

Inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents.

SCOPE

Organization-wide

RECOMMENDED ACTION

Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.

2.T LOG COLLECTION PR.PT-1

OUTCOME

Achieve better visibility to detect and effectively respond to cyberattacks.

TTP or RISK ADDRESSED

- Delayed, insufficient, or incomplete ability to detect and respond to potential cyber incidents
- Impair Defenses (T1562)

SCOPE

IT and OT assets

RECOMMENDED ACTION

Access- and security-focused logs (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network) are collected and stored for use in both detection and incident response activities (e.g., forensics). Security teams are notified when a critical log source is disabled, such as Windows Event Logging.

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

2.U SECURE LOG STORAGE PR.PT-1

OUTCOME

Organizations' security logs are protected from unauthorized access and tampering.

TTP or RISK ADDRESSED

- Indicator Removal on Host - Clear Windows Event Logs (T1070.001)
- Indicator Removal on Host - Clear Linux or Mac System Logs (T1070.002)
- Indicator Removal on Host - File Deletion (T1070.004)
- Indicator Removal on Host (ICS T0872)

SCOPE

IT and OT assets

RECOMMENDED ACTION

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.

2.V PROHIBIT CONNECTION OF UNAUTHORIZED DEVICES PR.PT-2

OUTCOME

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

TTP or RISK ADDRESSED

- Hardware Additions (T1200)
- Replication Through Removable Media (T1091, ICS T0847)

SCOPE

IT and OT 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 by limiting use of USB devices and removable media or disabling AutoRun.

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

2.W NO EXPLOITABLE SERVICES ON THE INTERNET PR.AC-3

OUTCOME

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

TTP or RISK ADDRESSED

- Active Scanning - Vulnerability Scanning (T1595.002)
- Exploit Public-Facing Application (T1190, ICS T0819)
- Exploitation of Remote Service (T1210, ICS T0866)
- External Remote Services (T1133, ICS T0822)
- Remote Services - Remote Desktop Protocol (T1021.001)

SCOPE

IT and OT assets on the public internet

RECOMMENDED ACTION

Assets on the public internet expose no exploitable services, such as remote desktop protocol. Where these services must be exposed, appropriate compensating controls are implemented to prevent common forms of abuse and exploitation. All unnecessary OS applications and network protocols are disabled on internet-facing assets.

2.X

LIMIT OT CONNECTIONS TO PUBLIC INTERNET

PR.PT-4, PR.AC-5

OUTCOME	TTP or RISK ADDRESSED	SCOPE	RECOMMENDED ACTION
Reduce the risk of threat actors exploiting or interrupting OT assets connected to the public internet.	• Active Scanning - Vulnerability Scanning (T1595.002) • Exploit Public-Facing Application (T1190, ICS T0819) • Exploitation of Remote Service (T1210, ICS T0866) • External Remote Services (T1133, ICS T0822)	OT assets on the public internet	No OT assets are on the public internet, unless explicitly required for operation. Exceptions must be justified and documented, and excepted assets must have additional protections in place to prevent and detect exploitation attempts (such as logging, MFA, mandatory access via proxy or other intermediary, etc.).

3.A– DETECTING RELEVANT THREATS AND TTPS

ID.RA-2, ID.RA-3, DE.CM-1

OUTCOME		RECOMMENDED ACTION
Organizations are aware of and able to detect relevant threats and TTPs.		Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
TTP or RISK ADDRESSED	**SCOPE**	
Without the knowledge of relevant threats and ability to detect them, organizations risk that threat actors may exist undetected in their networks for long periods.	N/A	

RESPOND

4.A– INCIDENT REPORTING

RS.CO-2, RS.CO-4

OUTCOME

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

TTP or 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 codified policy and procedures on to whom and how to report all confirmed cybersecurity incidents to appropriate external entities (e.g., state/federal regulators or SRMA's as required, ISAC/ISAO, as well as CISA).

Known incidents are reported to CISA as well as other necessary parties within time frames directed by applicable regulatory guidance or in the absence of guidance, as soon as safely capable. This goal will be revisited following full implementation of the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA).

4.B– VULNERABILITY DISCLOSURE/REPORTING

RS.AN-5

OUTCOME

Organizations more rapidly learn about vulnerabilities or weaknesses in their assets discovered by security researchers; researchers are more incentivized to responsibly share their findings.

TTP or RISK ADDRESSED

- Active Scanning - Vulnerability Scanning (T1595.002)
- Exploit Public-Facing Application (T1190, ICS T0819)
- Exploitation of Remote Service (T1210, ICS T0866)
- Supply Chain Compromise (T1195, ICS T0862)

SCOPE

All assets

RECOMMENDED ACTION

Consistent with NIST SP 800-53 Revision 5, organizations maintain a public, easily discoverable method for security researchers to notify (e.g., via email address or web form) organizations' security teams of vulnerable, misconfigured, or otherwise exploitable assets. Valid submissions are acknowledged and responded to in a timely manner, taking into account the completeness and complexity of the vulnerability. Validated and exploitable weaknesses are mitigated consistent with their severity.

Security researchers sharing vulnerabilities discovered in good faith are protected under Safe Harbor rules.

In instances where vulnerabilities are validated and disclosed, public acknowledgement is given to the researcher who originally submitted the notification.

4.C– DEPLOY SECURITY.TXT FILES

RS.AN-5

OUTCOME

Allow security researchers to submit discovered weaknesses or vulnerabilities faster.

TTP or RISK ADDRESSED

- Active Scanning - Vulnerability Scanning (T1595.002)
- Exploit Public-Facing Application (T1190, ICS T0819)
- Exploitation of Remote Service (T1210, ICS T0866)
- Supply Chain Compromise (T1195, ICS T0862)

SCOPE

All public-facing web domains

RECOMMENDED ACTION

All public-facing web domains have a security.txt file that conforms to the recommendations in RFC 9116.

5.A– INCIDENT PLANNING AND PREPAREDNESS

RC.RP-1, PR.IP-9, PR.IP-10

OUTCOME	TTP or RISK ADDRESSED	SCOPE	RECOMMENDED ACTION
Organizations are capable of safely and effectively recovering from a cybersecurity incident.	Disruption to availability of an asset, service, or system.	IT and OT assets	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident.

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.

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

Assets: A person, structure, facility, information, material, or process that has value.

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.

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

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.

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.

Continuous Monitoring: Maintaining ongoing awareness to support organizational risk decisions.

Common Vulnerabilities and Exposures (CVE): A nomenclature and dictionary of security-related software flaws.

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.

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, distributed control system (SCADA), programmable logic controllers (PLCs), and other types of industrial measurement and control systems.

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 Lifecycle: Federal agencies are heavily dependent upon their information and information systems to successfully conduct critical missions. With an increasing reliability on and growing complexity of information systems, as well as a constantly changing risk environment, information security has become a mission-essential function. This function must be conducted in a manner that reduces the risks to the information entrusted to the agency, its overall mission, and its ability to do business and to serve the American public. Information security is a business enabler when applied through proper and effective management of risks to information confidentiality, integrity, and availability.

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 cyberattacks against an organization's information systems(s).

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.

Demilitarized Zone (DMZ): 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.

Encrypt: Cryptographically transform data to produce cipher text.

Encryption: Any procedure used in cryptography to convert plain text into cipher text to prevent anyone but the intended recipient from reading that data.

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.

Firmware: Software program or set of instructions programmed on the flash ROM of a hardware device. It provides the necessary instructions for how the device communicates with the other computer hardware.

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.

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.

Incident Response Plan: A set of predetermined and documented procedures to detect and respond to a cyber incident.

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.

Information Sharing and Analysis Centers (ISACs): A trusted operational entity established by private sector critical infrastructure owners and operators in consultation with and with assistance from the federal government (as requested) to serve as a mechanism for gathering, analyzing, appropriately sanitizing, and disseminating information about vulnerabilities, threats, intrusions, and anomalies to industry and government partners. ISACs operate through a sector-based model; facilities and organizations within a particular critical infrastructure sector collaborate to share information and best practices about physical and cyber threats and mitigation strategies. Most ISACs maintain situational awareness of their sectors and provide threat warning and incident reporting 24 hours a day, 7 days a week; some also set the threat level for their sectors. While crucial to successful public-private partnerships, ISACs are not intended to interfere with direct exchanges of information between individual companies and the government.

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.

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.

International Society of Automation (ISA): The International Society of Automation (ISA) is 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.

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).

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 cyberattacks.

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.

Logs: A record of the events occurring within an organization's systems and networks.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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

Phishing-Resistant MFA: As defined in OMB 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.

Privileged Accounts: An information system account with approved authorizations of a privileged user.

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, login to servers, and to perform other remote actions. Remote users use RDP to log into the organization's network to access email and files.

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.

System Architecture: An architecture is the fundamental organization of a system, embodied in its components, their relationships to each other and the environment, and the principles governing its design and evolution.

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.

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.

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

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; Pacific Northwest National Laboratory (PNNL); 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.