Mitigation Guide: Healthcare and Public Health (HPH) Sector

October 2023
Cybersecurity and Infrastructure Security Agency

This document is marked TLP:CLEAR. Recipients may share this information without restriction. Information is subject to standard copyright rules. For more information on the Traffic Light Protocol, see http://www.cisa.gov/tlp.

Contents

Introduction

This Cybersecurity and Infrastructure Security Agency (CISA) Mitigation Guide offers recommendations and best practices to combat pervasive cyber threats affecting the Healthcare and Public Health (HPH) Sector. Identified vulnerabilities in organizations across the HPH Sector present opportunities to mitigate risks before intrusions occur. Unmitigated vulnerabilities increase the likelihood of threat actors successfully employing malicious tactics, techniques, and procedures (TTPs) against HPH organizations.

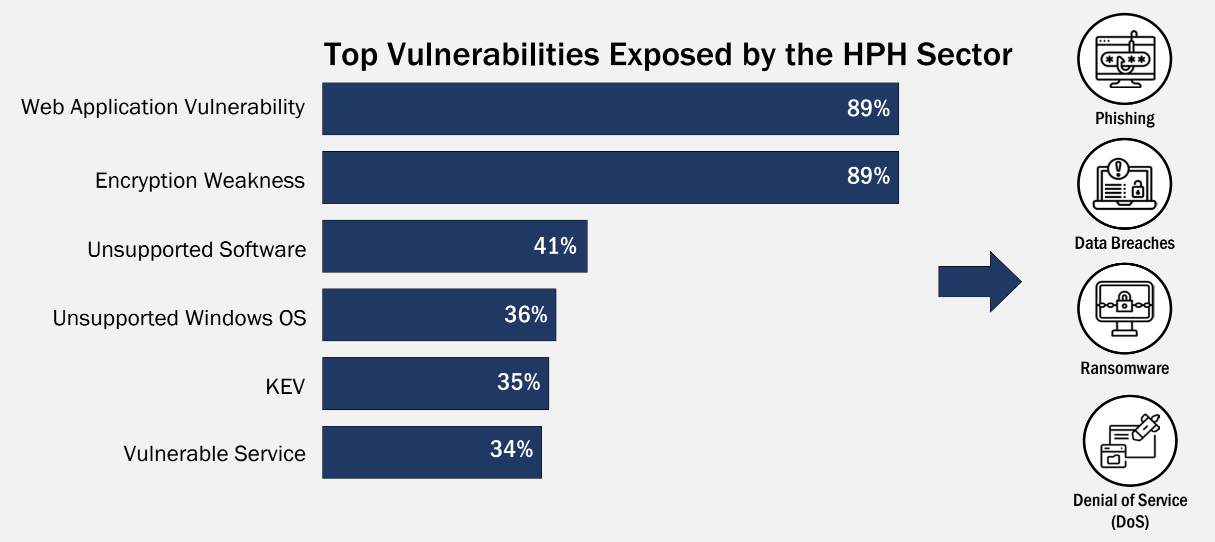

Figure 1: Key Vulnerabilities and Threats to the HPH Sector

As indicated in the ***Cyber Risk Summary: Healthcare and Public Health (HPH) Sector Calendar Year 2022***[1] and figure 1, CISA identified common vulnerabilities and insecure configurations across the HPH Sector, such as:

- Web application vulnerabilities
- Encryption weaknesses
- Unsupported software
- Unsupported Windows operating systems (OS)
- Known exploited vulnerabilities (KEVs)
- Vulnerable services[2]

Exposure of these vulnerabilities can result in detrimental cyber activity, such as ransomware, data breaches, or denial-of-service. Each of these can compromise the availability, confidentiality, and integrity of critical HPH systems, functions, and data.

This vulnerability mitigation guidance maps CISA's Cross-Sector Cybersecurity Performance Goals (CPGs) to Health and Human Services (HHS) and the Health Sector Coordinating Council's (HSCC) joint publication: 405(d) Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients which is detailed in the CPG HICP Crosswalk guide. This mitigation guide evaluates the most common vulnerabilities exposed in the HPH Sector and provides tailored recommendations and best practices for HPH organizations of all sizes. In addition to CPGs, HICPs, and the HPH Sector Cybersecurity Framework Implementation Guide, CISA recommends manufacturers of HPH technology products take actions in line with CISA's Principles and Approaches for Security-by-Design and -Default in order to reduce the burden of cybersecurity on their customers.

[1] The *Cyber Risk Summary: Healthcare and Public Health (HPH) Sector Calendar Year 2022* is a TLP:GREEN report; authorized recipients may contact their regional cybersecurity advisor or csd_vm_insights_intake@cisa.dhs.gov for access.
[2] Refer to Table 3 in the *Mitigation Strategy #1 Asset Management and Security* section below for more information on the vulnerable services.

Data Note

The HPH Cyber Risk Summary and this Mitigation Guide evaluates and analyzes vulnerability data from internet-accessible assets of HPH Sector entities enrolled in CISA's Cyber Hygiene (CyHy) Vulnerability Scanning (VS) and Web Application Scanning (WAS) services. To contextualize vulnerability trends and to help HPH entities further understand the threats and risks to their sector, this guide incorporates CISA's KEV catalog, open-source information, commercial threat intelligence feeds, and the MITRE ATT&CK® (Adversarial Tactics, Techniques, and Common Knowledge) framework.

Additionally, this guide provides recommended mitigation guidance with baseline mitigations mapped to CISA's CPGs. Using similar sourcing, this guide provides additional guidance and support to HPH entities by leveraging and expanding on data presented by the Cyber Risk Summary for the HPH Sector.[1] Table 1 shows each of the sources and frameworks used throughout this document.

Table 1: Sources and Frameworks[3]

Source	Owner	Description
Cyber Hygiene (CyHy) Vulnerability Scanning (VS)	CISA	CyHy VS evaluates external network presence by executing continuous non-credentialed scans of public, internet-facing, static IPv4s for accessible services and vulnerabilities using NMAP and Tenable Nessus.
Web Application Scanning (WAS)	CISA	WAS is "internet scanning-as-a-service" that assesses the "health" of publicly accessible web applications by checking for known vulnerabilities and weak configurations.
Cross-Sector Cybersecurity Performance Goals (CPGs) Version 1.0.1	CISA	The CPGs are a prioritized subset of IT and OT cybersecurity practices that critical infrastructure owners and operators can implement to meaningfully reduce the likelihood and impact of known risk and adversary techniques.
Health Industry Cybersecurity Practices (HICP)	HHS/H SCC	The HICP publication provides a starting point with ten mitigating practices for implementing basic cybersecurity practices in healthcare organizations.
CPG HICP Crosswalk	HHS/H SCC	Mapping designed to be utilized as a pathway to connect CISA's CPGs to HHS 405(d)'s HICP publication.
MITRE ATT&CK Framework Version 13.0	MITRE	The MITRE ATT&CK framework is a guideline for classifying and describing cyberattacks and intrusions.
Known Exploited Vulnerability (KEV) Catalog	CISA	The KEV catalog is a prioritized set of vulnerabilities that have been actively exploited in the wild.

[3] Some descriptions are taken directly from source sites.

Mitigation Strategy #1 Asset Management and Security

Due to the high value of protected health information (PHI) and the criticality of patient-focused services, threat actors continuously look for new ways to exploit vulnerabilities within the HPH Sector. Organizations that have not implemented or maintained an asset management policy risk exposing vulnerabilities or services that could be exploited by threat actors to gain unauthorized access, steal sensitive data, disrupt critical services, or deploy ransomware, causing significant harm to patients and the organization's reputation.

This section addresses different concepts of asset management and asset security, including asset inventory, procurement, decommissioning, and network segmentation, as they relate to hardware, software, and data assets.

Focus Area 1: Asset Inventory

As an initial and priority mitigation strategy, CISA recommends implementing and maintaining an inventory of assets for your environment. Knowing which assets are on your organization's network is fundamental to cybersecurity: "you can't secure what you can't see." Cybersecurity professionals within the HPH Sector should identify and understand all relationships or interdependencies, functionality of each asset, what it exposes, and what software is running to make sure every organization protects electronic PHI (ePHI) and enables Health Insurance Portability and Accountability Act (HIPAA) compliance. Organizations can complete asset inventories using active scans, passive processes, or a combination of both techniques. Collection of the asset inventory attributes listed in figure 2 will illuminate your network, so you can manage your inventory.

Vulnerabilities and Threats Addressed

- KEVs
- Vulnerable services
- Outdated and unsupported software and OS
- Ransomware attacks
- Loss or theft of equipment/data
- Attacks against network connected medical devices

Associated MITRE ATT&CK Techniques

- T1021 Remote Services
- T1046 Network Service Discovery
- T1133 External Remote Services
- T1190 Exploit Public-Facing Application
- T1199 Trusted Relationship
- T1210 Exploitation of Remote Services
- T1219 Remote Access Software
- T1482 Domain Trust Discovery
- T1563 Remote Service Session Hijacking
- T1557 Adversary-in-the-Middle
- T1571 Non-Standard Port
- T1610 Deploy Container

Relevant CISA CPG and HHS HICP

- Asset Inventory - CPG 1.A | HICP 5.M.A
- Network Segmentation - CPG 2.F | HICP 6.M.A
- OT Cybersecurity Training - CPG 2.J | HICP 10.S.C
- Secure Sensitive Data - CPG 2.L | HICP 1.M.A
- Hardware and Software Approval Process - CPG 2.Q | HICP 2.L.D
- Prohibit Connections of Unauthorized Devices - CPG 2.V | HICP 2.S.A
- No Exploitable Services on the Internet - CPG 2.W | HICP 3.S.A
- Limit OT Connections to the Public Internet - CPG 2.X | HICP 6.S.A

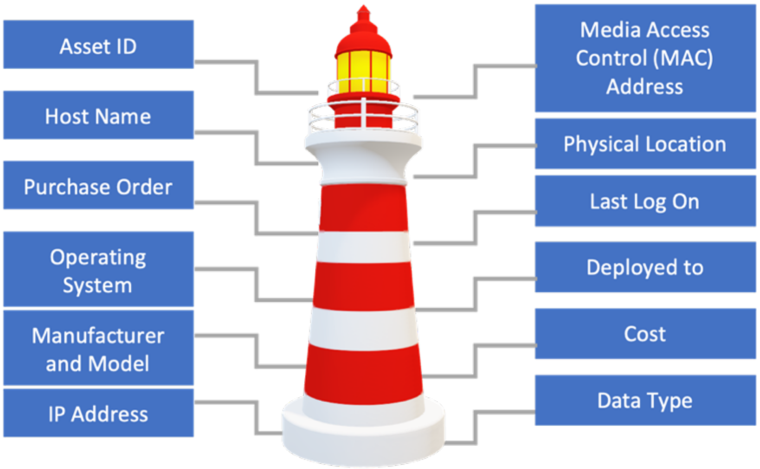

Figure 2: Asset Inventory Attributes

- Active discovery tools, including network monitoring tools with automated discovery functionality, scan the network with a variety of different packet types to identify all assets connected. Active asset discovery is usually more reliable than passive; however, it can cause network congestion or interrupt sensitive devices. Active asset discovery techniques could also negatively impact older medical devices due to their limited memory and central processing unit (CPU).
- Passive discovery techniques include reviewing logs from switches, routers, active directory, and elsewhere to identify network assets. Although these techniques are considered less disruptive to your network, they tend to miss assets that have not generated any activity during the review period.
- Hybrid discovery uses both active and passive asset techniques, as appropriate, throughout the network. Hybrid discovery depends on a solid understanding of organizational network structure to inform design and implementation.

CISA recommends tasking designated personnel within your organization with maintaining the inventory by updating, tracking, and adding or removing assets—especially during procurement or decommissioning stages. CISA encourages HPH entities to codify the procurement and decommission of assets and technology into a standard operating procedure (SOP), assigning roles and responsibilities for each function.

Outdated technology or IT assets no longer in use should be securely stored (e.g., lockers, cages, rooms) or decommissioned according to the organization's policies and procedures. Although decommissioning assets may sound like a stress-free task, CISA encourages organizations to work with outside vendors specializing in secure destruction or wiping.[4] Be sure to obtain a receipt of destruction and disposal from the vendor to avoid abuse or misuse of data on decommissioned assets.

[4] Ilascu, Ionut. "Hackers Can Breach Networks Using Data on Resold Corporate Routers." BleepingComputer. April 23, 2023. https://www.bleepingcomputer.com/news/security/hackers-can-breach-networks-using-data-on-resold-corporate-routers/.

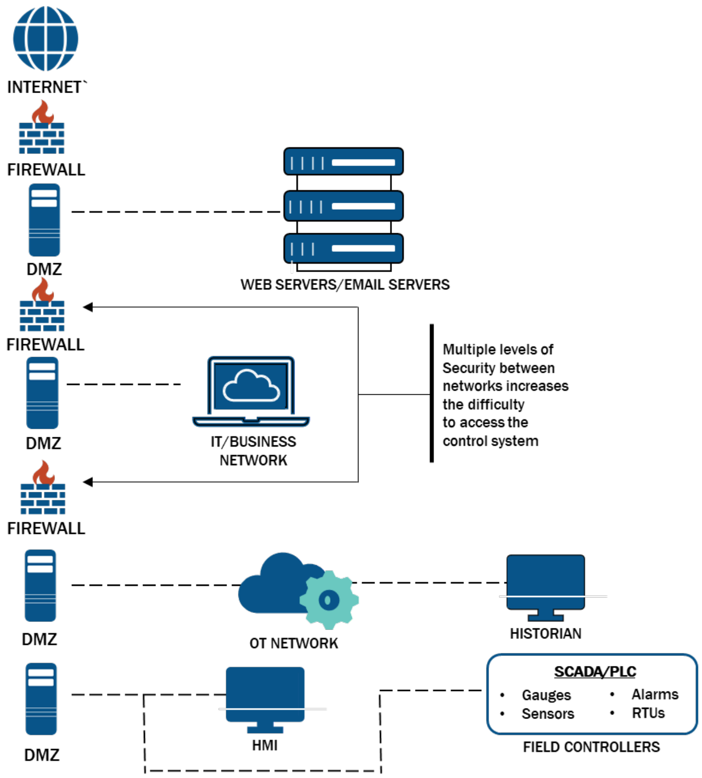

Figure 3: Network Segmentation

Focus Area 2: Securing Your Assets

Upon the creation of your asset inventory, CISA recommends implementing network segmentation to isolate IT and OT devices onto different segments.[5] Network segmentation divides a network into smaller parts, enabling control over cross-segment network communication. An important component of network security is controlling which assets can access OT networks, which assets can access the internet from an internal network, and which assets should be siloed into their own compartment.

As seen in figure 3, demilitarized zones (DMZs) and firewalls shield the network from unauthorized access, with firewalls capable of blocking traffic from network addresses, applications, or ports while allowing necessary data through. Policies and controls should be used to monitor and regulate system access and the movement of traffic between zones.

In the event of a breach or compromise, properly secured network segments can prevent threat actors from moving laterally through your environment. A well-maintained asset inventory helps detail how network administrators divide resources into segments based on a set of considerations, including the criticality of the asset to business functions, the sensitivity of the data traversing the asset, and the requirements of internet access to the asset. Table 2 shows network segmentation controls.

[5] National Institute of Standards and Technology (NIST). “Special Publication 800-82 Rev. 2 Guide to Industrial Control Systems (ICS) Security.” NIST. May 2015. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

Table 2: Network Segmentation Controls

	Network Segmentation Control	Description
☑	**Establish and Maintain a Network Architecture**	Provides a detailed view of assets and network architecture.
☑	**Configure Firewalls and Access Control Lists (ACLs)**	Approves or denies cross-segment communications based on network administrator rules.
☑	**Collect and Analyze Traffic Logs**	Determine monitoring strategy depending on resources available to inspect cross-segment communication.

While technological advances in medical devices reduce labor burden and exposure to human error, network-connected devices introduce new cybersecurity vulnerabilities that may bring greater risks, adversely affecting patient care. Traditional IT devices like switches, routers, and servers may not have been designed with security in mind, however, such devices can be integrated and managed by most security tools, if properly configured.

Technologies used in healthcare environments often share the same design principles and could expose vulnerable services that threat actors could leverage at any point in the cyber kill chain. In November 2022, the Federal Bureau of Investigation (FBI), CISA, and the Department of Health and Human Services (HHS) released a cybersecurity advisory (CSA) indicating that the Hive ransomware group gains initial access to victim networks using Remote Desktop Protocol (RDP), virtual private networks (VPN), and other remote network connection protocols.[6] Table 3 lists vulnerable and exploitable services and their associated common port.

Table 3: Vulnerable and Exploitable Services

Category	Services (Common Ports)
Remote Access	RDP (3389), Telnet (23)
File Transfer/File Sharing	FTP (20, 21), SMB (445)
Inter-Process Communications	RPC (135), NetBIOS (137, 138), SNMP (161, 162)
Authentication and Authorization	Kerberos (88, 464), LDAP (389)
Database	SQL (1433)

[6] Cybersecurity and Infrastructure Security Agency. “#StopRansomware: Hive Ransomware.” Cybersecurity and Infrastructure Security Agency. November 17, 2022. https://www.cisa.gov/sites/default/files/publications/aa22-321a_joint_csa_stopransomware_hive.pdf

CISA recommends HPH entities implement the mitigations listed in table 4 across their entire infrastructure to limit exposure.

Table 4: Asset Security Mitigations

	Mitigation Category	Recommended Mitigation
☑	**Port and Service Exposure**	• Minimize network exposure to only those services required by organization need. • Disable unused or unnecessary ports on switches, using the switchport security feature. • Protect the exposure of vulnerable services by business need by requiring access with phishing-resistant multifactor authentication (MFA). • Maintain updated versions of exposed services and remove outdated and unsupported versions.
☑	**Network and Security Monitoring**	• Implement network segmentation to separate and restrict communications between publicly exposed endpoints and the internal network. • Ensure signature-based intrusion detection systems (IDS) have their signature sets updated regularly.
☑	**Database Security**	• Revoke “execute” function on generous Structured Query Language (SQL) server functions. • Ensure unvalidated statements are not included within your “allowed” statements. • Define SQL code with prepared statements to differentiate between code and user input. • Ensure up-to-date notification agreements with third-party vendors are completed.

Resources

- 405(d) Prescription Poster: Asset Management
- NIST Special Publication 1800-5B: IT Asset Management
- NIST Special Publication 800-82 rev 2: Guide to Industrial Control Systems (ICS) Security
- SANS ICS Concepts Video: Building a Secure OT Network
- NIST Special Publication 800-41 rev 1: Guidelines on Firewalls and Firewall Policy
- HHS HPH Sector Cybersecurity Framework Implementation Guide
- CISA Binding Operational Directive 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks

Mitigation Strategy #2 Identity Management and Device Security

As the HPH Sector continues to transition more of its assets and systems online, CISA recommends entities secure their devices and digital accounts and manage their online access to protect sensitive data and PHI from compromise.

Several key areas discussed in this section include email security and phishing prevention, access management and monitoring, password policies, and data protection practices.

Focus Area 1: Email Security and Phishing Prevention

With the continued threat of phishing emails and business email compromise (BEC) attacks, it is essential for organizations to properly configure and secure their email systems. Additionally, to remain in compliance, organizations must apply the appropriate email safeguards to meet the HIPAA Security Rule requirements, which protect ePHI.

Organizations should ensure modern anti-malware software is installed and signatures are automatically updated where possible. For additional guidance, see CISA's Enhance Email and Web Security Guide.

To optimize email security and protection, CISA recommends implementing all email security controls noted in table 5. These email protection controls are also recommended by Software as a Service (SaaS) email services such as Microsoft O365 and Google Workspace. The HIPPA Journal's, Office 365 Email Security blog and Google Workspace's Help prevent spoofing, phishing, and spam help center repository offer detailed email protection guidance.

Vulnerabilities and Threats Addressed

- Web Application Vulnerabilities
- Phishing Attempts
- Ransomware Attacks
- Social Engineering
- Data breaches

Associated MITRE ATT&CK Techniques

- T1098 Account Manipulation
- T1078 Valid Accounts
- T1566 Phishing
- T1110 Brute Force
- T1557 Adversary-in-the-Middle
- T1565 Data Manipulation
- T1003 OS Credential Dumping

Relevant CISA CPG and HHS HICP

- Changing Default Passwords - CPG 2.A | HICP 9.M.B
- Minimum Password Strength - CPG 2.B | HICP 3.M.C
- Unique Credentials - CPG 2.C | HICP 3.M.C
- Revoking Credentials for Departing Employees - CPG 2.D | HICP 3.S.A
- Separating User and Privileged Accounts - CPG 2.E | HICP 2.S.A
- Detection of Unsuccessful (Automated) Login Attempts - CPG 2.G | HICP 2.M.B
- Phishing-Resistant Multifactor Authentication (MFA) - CPG 2.H | HICP 2.M.A
- Basic Cybersecurity Training - CPG 2.I | HICP 10.S.C
- Strong and Agile Encryption - CPG 2.K | HICP 2.S.A and 1.M.B
- Secure Sensitive Data - CPG 2.L | HICP 1.M.A
- Email Security - CPG 2.M | HICP 1.M.A
- Log Collection - CPG 2.T | HICP 2.L.B
- Secure Log Storage - CPG 2.U | HICP 6.L.A

Table 5: Email Protection Controls

	Email Control	Description
☑	**Enable StartTLS**	Command used to upgrade an existing non-encrypted connection to an encrypted one.
☑	**Implement Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM)**	Allows a sending domain to "watermark" their emails, making unauthorized emails easy to detect.
☑	**Set Domain-Based Message Authentication Reporting and Conformance (DMARC) to "reject"**	Ensures that unauthenticated messages are rejected at the mail server, even before delivery.

Organizations should establish and maintain a cybersecurity training program for the workforce covering basic cybersecurity concepts, such as phishing awareness, business email compromise, basic operational security, and password security. At minimum, the training should occur annually, and new employees should receive initial cybersecurity training within the first 10 days of onboarding.

Employees should take extra care when sending and receiving emails containing PII or PHI, double checking the email address of the intended recipient of the email is correct.

Table 6 shows what employees should recognize as examples of phishing techniques and indicators.

Table 6: Example of Phishing Techniques and Indications

	Indicator	Description
🔗	**Check for embedded or spoofed hyperlinks**	Validate the URL of the link matches the text of the link itself. This can be achieved by hovering your cursor over the link to view the URL of the website to be accessed. Always be careful when clicking on an external link, as not all external links will direct you to a trusted website.
✉	**Look for suspicious "From:" addresses**	Check received emails for spoofed or misspelled "From:" addresses. You can check this by hovering over the sender's name. Legitimate addresses should match what is in the "From:" field.
⚠	**Be cautious with "urgent" messages**	If the email message requires immediate action, especially if it includes a request to access your email or any other account, do not open the email or take any action without verifying that it is legitimate.
🐷	**Be cautious with" too good to be true" messages**	If you receive an unexpected message about winning money or gift cards, do not open the email or take any action without verifying that it is legitimate.
✕	**Be cautious of misspellings, grammar mistakes, or layout errors**	Check received emails for any spelling or grammar mistakes, or layout errors. It is unusual to see mistakes like these in a legitimate email.

For additional information and guidance on phishing, see CISA's Phishing Infographic.

Focus Area 2: Access Management

Just as personnel may use a name badge to identify themselves in the physical work environment, cybersecurity access management practices are essential for ensuring all users are properly identified and authenticated in the digital space. For basic access management, organizations should implement the following:

- **Implement MFA, ideally phishing-resistant MFA.** MFA is a layered approach to securing online accounts and devices. MFA requires a combination of two or more authenticators to verify a user's identity before the service grants access, with the additional factor as something you have, something you are, or something you know. Phishing-resistant MFA completes the same process but removes 'people' from the equation to help thwart social engineering scams and targeted phishing attacks that may have been successful using traditional MFA. The two main forms of phishing-resistant MFA are FIDO/Web Authentication (WebAuthn) authentication and Public Key Infrastructure (PKI)-based authentication. Prioritize phishing-resistant MFA on accounts with the highest risk, such as privileged administrative accounts on key assets. For additional information on phishing-resistant MFA, see CISA's Implementing Phishing-Resistant MFA Guide.

- **Maintain unique and separate accounts for each user in your organization.** Users should not share passwords. Each user should create an account password that is different from their personal accounts. Avoid the use of shared or generic accounts, where possible.

- **Terminate access as soon as a user leaves your organization.** If a user changes roles within the organization, it is important to terminate access from their former position before issuing new credentials.

- **Restrict the use of elevated privileged accounts.** Organizations should issue system administrators two accounts: one with elevated privileges and another for routine office functions (such as web browsing or business email). Be sure to conduct a periodic review of all privileged access and accounts.

Focus Area 3: Password Policies

The creation of strong and unique credentials and passwords is vital to account and device security. Threat actors have leveraged weak and shared credentials to gain initial network access and carry out various attacks. Organizations should seek to implement the following:

- **Change all default passwords.** Before placing any hardware, software, or firmware on your network, immediately change any vendor-supplied default passwords.

- **Password length should be a minimum of 15 characters.** To make passwords harder for threat actors to guess or crack, organizations should require a minimum password length of 15 or more characters where technically feasible. For more guidance on how to create secure passwords, see CISA's Creating a Password guidance.

Focus Area 4: Data Protection and Loss Prevention

With HIPAA requirements to protect patient health information, any data or security breach resulting in the compromise, loss, or disclosure of sensitive data, including PII and PHI, can have major impacts for your organization. To prevent disruption to patient safety and the provision of care, it is essential for all HPH entities to implement good data protection policies that ensure the security of sensitive information. For data protection and loss prevention, organizations should implement the following:

- **Ensure proper storage and access management for all sensitive information, including credentials.** Sensitive data, such as credentials, should not be sorted in plaintext, and should only be accessed by authenticated and authorized users. Consider privileged account management solutions, such as a credential/password manager, to ensure all credentials are securely stored.

- **Maintain strong and updated encryption protocols and algorithms.** Organizations should ensure properly configured and up-to-date encryption protocols, such as transport layer security (TLS), are utilized to protect data, both at rest and in-transit. Organizations should also plan to identify any use of outdated or weak encryption ciphers, and update these to sufficiently strong algorithms.

Table 7 shows additional encryption best practices.

Table 7: Encryption Best Practices

	Encryption Practice	Description
☑	**Key Algorithm**	Depending on the use case and sensitivity of the data, either a symmetric algorithm, such as Advanced Encryption Standard (AES), or an asymmetric algorithm, such as RSA or Elliptic Curve Digital Signature Algorithm (ECDSA) should be selected. Symmetric algorithms use the same key for both encrypting and decrypting the data, while asymmetric encryption algorithms use two different keys.
☑	**Key Size**	NIST recommends 256 bits for AES keys and 2048 or 4096 bits for RSA keys. For key size, the larger the key the more secure it is and the longer it will provide protection. However, since larger keys can also result in performance issues, the size choice should be made carefully given the use case.
☑	**Crypto Agility**	Encryption algorithms tend to get weaker over time. It is important for your organization be prepared to change algorithms and/or key sizes. Be aware of the threat of quantum computing and be prepared to shift to post-quantum algorithms if/when necessary.
☑	**Key Rotation**	Using the same key over a long duration of time increases the chances that the key will be compromise. It is good practice to update (or rotate) encryption keys periodically.
☑	**Key Retirement**	When a key is no longer required, the key should be retired. Retirement involves permanently deleting the key to ensure there is no further risk and to reduce the number of active keys being managed.
☑	**Secure Key Storage**	NIST recommends using a Hardware Security Module (HSM) to store encryption keys, as these provide strong physical and logical protection.
☑	**Access Control**	Encryption keys should not be available to all users at any time. Only authorized and authenticated users should be allowed to access, manage, and use the encryption keys.

Focus Area 5: Device Logs and Monitoring Solutions

To protect devices and prevent threat actors from moving laterally through your organization's network, consider implementing an endpoint detection and response (EDR) solution. An EDR is an endpoint security solution that continuously monitors end-user devices to detect suspicious behavior, provide contextual information, and respond with remediation suggestions.

When selecting an EDR solution, ensure it incorporates user and entity behavior analytics (UEBA) and closely monitor access logs to detect deviations outside of normal behavior. Unsuccessful or automated login attempts should be logged. Store logs in a central system, such as a security information and event management (SIEM) tool or central database. Logs should only be accessed or modified by authorized and authenticated users and should be securely stored for a duration that is recommended by risk or regulatory guidelines.

Resources

- CISA Multifactor Authentication
- CISA Phishing Infographic
- NIST SP 800-63-3 Digital Identity Guidelines
- H-ISAC Introduction and Email Protection Systems Cybersecurity for the Clinician Training
- H-ISAC Data Protection and Loss Prevention Cybersecurity for the Clinician Training
- HHS Technical Volume 1: Cybersecurity Practices for Small Healthcare Organizations
- HHS Technical Volume 2: Cybersecurity Practices for Medium and Large Healthcare Organizations
- HHS HPH Sector Cybersecurity Framework Implementation Guide

Mitigation Strategy #3 Vulnerability, Patch, and Configuration Management

Focus Area 1: Vulnerability and Patch Management

Vulnerability management is the ongoing process of identifying, assessing, reporting on, managing, and remediating cyber vulnerabilities in software and systems. The process involves proactively scanning devices and systems for vulnerabilities or technology flaws that threat actors could exploit. Often used interchangeably with vulnerability management, patch management is a vital component of every vulnerability management solution. Patch management involves applying updates to servers, applications, and software to address security flaws. Vulnerability and patch management are key components in planning for and determining the appropriate implementation of controls and the management of risk.

As vulnerability management is a continuous and evolving process, it is often a multi-step cycle, as depicted in figure 4.

Vulnerabilities and Threats Addressed

- KEVs
- Ransomware attacks
- Data breaches

Associated MITRE ATT&CK Techniques

- T1190 Exploit Public-Facing Application
- T1210 Exploitation of Remote Services
- T1212 Exploitation for Credential Access

Relevant CISA CPG and HHS HICP

- Mitigating Known Vulnerabilities - CPG 1.E | HICP 7.M.D and 2.S.A
- Document Device Configurations - CPG 2.O | HICP 10.S.B
- Detecting Relevant Threats and TTPs - CPG 3.A | HICP 2.L.B

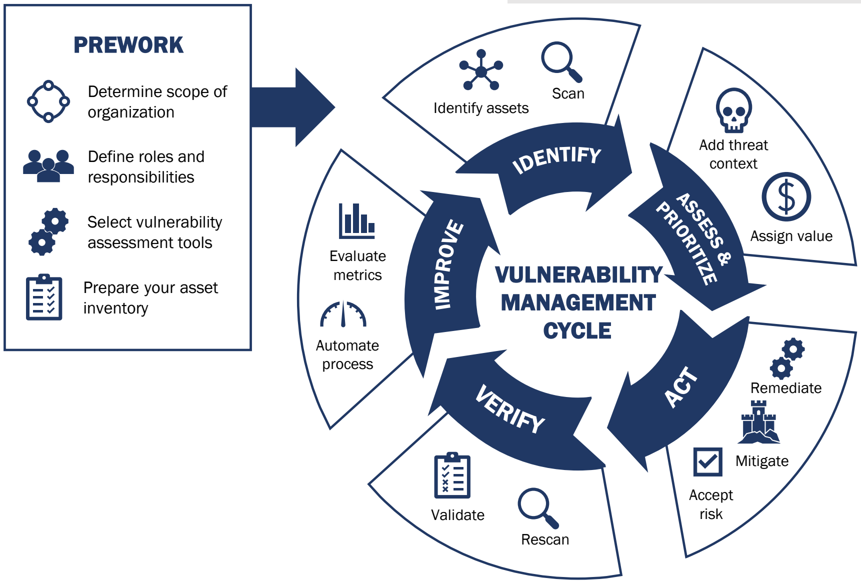

Figure 4: Vulnerability Management Lifecycle
(adapted from the Gartner Vulnerability Management Guidance Framework)

Step 1. Identify. The first and most important step in any vulnerability management process is to identify all vulnerabilities that may exist in your organization's environment. To help discover the vulnerabilities, follow these steps:

- **An Asset Inventory.** An asset inventory should list all your organization's enterprise assets, such as devices, operating systems, software, and services that will be assessed for vulnerabilities.

- **A Vulnerability Scanner.** A vulnerability scanner conducts credentialed and uncredentialed scans of network-accessible systems, identifying open ports and services running on those scanned systems, and looks for any known vulnerabilities when configured properly. CISA offers free vulnerability scanning via Cyber Hygiene (CyHy) Services for internet-facing assets. HPH entities should use a vulnerability scanner configured with up-to-date plugins to perform continuous scans on internal network assets.

Step 2. Assess and Prioritize. Once vulnerabilities are identified across your environment, evaluate and prioritize to appropriately deal with the posed risks according to your organization's risk strategy. To assist with prioritization, it is essential to:

- **Map your assets to business-critical functions.** For vulnerability remediation, prioritize assets that are most critical for ongoing operations or which, if affected, could impact your organization's business continuity, sensitive PII or PHI security, reputation, or financial position.
- **Use threat intelligence information.** For remediation, prioritize vulnerabilities actively exploited by threat actors. To assist, leverage CISA's KEV Catalog and other threat intelligence feeds.
- **Leverage prioritization methodologies, ratings, and scores.** The Common Vulnerability Scoring System (CVSS) assesses the technical severity of vulnerabilities. The Exploit Prediction Scoring System (EPSS) measures the likelihood of exploitation and can help with deciding which vulnerabilities to prioritize. CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) methodology leverages decision trees to prioritize relevant vulnerabilities into four decisions, Track, Track*, Attend, and Act based on exploitation status, technical impact, mission prevalence, and impacts to safety and public-wellbeing.

Step 3. Act. Once a vulnerability has been assessed and deemed a risk, it must be treated. When determining specific treatment strategies, it is best for an organization's security team, system owners, and system administrators to come together and determine the appropriate remediation approach. There are three actions organizations can take for an identified vulnerability:

- **Remediation.** Remediation involves fully fixing or patching a vulnerability so threat actors cannot exploit it. Remediation is the ideal treatment option organizations should strive for.
- **Mitigation.** Mitigation lessens the likelihood and/or impact of a vulnerability being exploited. This can be necessary when a proper fix or patch is not yet available for an identified vulnerability. Ideally, mitigation should be used to buy time for an organization to eventually remediate a vulnerability.
- **Acceptance.** Acceptance involves taking no action to fix or lessen the likelihood and/or impact of a vulnerability being exploited. This is typically justified when a vulnerability is deemed a low risk or the cost of or risk inherent in fixing the vulnerability is much greater than the cost or outcome incurred by an organization if the vulnerability were to be exploited.

To assist with vulnerability prioritization and treatment, use CISA's Stakeholder-Specific Vulnerability Categorization (SSVC) Guide and SSVC Calculator.

Step 4. Verify. Once remediation is considered complete, it is wise to run another vulnerability scan to ensure the vulnerability has in fact been effectively remediated or mitigated.

Step 5. Improve. To improve and refine your vulnerability management process, continue to perform regular vulnerability assessments, and evaluate the results, making any necessary adjustments to enhance the speed and efficiency of your program.

To get the most out of your organization's vulnerability management program, it is best practice to scan all software, devices, and systems at least monthly. Organizations should continually assess vulnerability exposure, maintain robust documentation of all vulnerability scans, and implement patches that are produced by the vendor community.

Focus Area 2: Configuration and Change Management

Alongside established vulnerability and patch management solutions, HPH entities should implement security configuration management (SecCM) to identify and address misconfigurations in default system settings. This process involves identifying, controlling, accounting for, and auditing changes made to pre-established baselines, with the goal of moving beyond the original design of a system, to a hardened, operationally sound version. Like vulnerability management, configuration and change management (CCM) follows several cyclical steps:

Step 1. Identify configuration items. Leveraging your asset inventory, this step involves identifying the configuration items (e.g., hardware, software, or firmware) within your organization's environment that require management. Maintain documentation of basic attributes, such as make/model, serial number, operating system, location, and owner.

Step 2. Establish secure baselines. As vendor default settings are rarely secure and often targeted by threat actors, it is essential that entities have pre-established secure configuration baselines. Vendors can help by providing secure by default configurations, ensuring that their product is secure out of the box. Organizations can leverage the benchmarks from trusted institutions, such as CIS or NIST (see Resources below), to develop their baselines, which should include the minimum tasks to:

- Disable unnecessary services and ports.
- Install the latest system and security patches.

Rename default system accounts.

- Change default passwords/credentials.
- Configure MFA where possible and appropriate.
- Enable security configurations, such as internal firewalls and automatic updates.

Step 3. Implement and audit changes. Once an organization identifies configurations and establishes baselines, it can apply changes to the systems. Consider using automated tools to apply the configurations where possible; automation lowers the risk of incorrectly applying configurations and provides an audit trail of all changes to prevent unauthorized actions.

Step 4. Assess and remediate. Configuration management is a cyclical process; it is important to ensure changes are continually assessed and remediated. Entities should consult their vulnerability management strategy and run assessments to verify expected changes were successful or remediate if not.

Resources

- CISA Cyber Resilience Review Supplemental Resource Guide Volume 4 Vulnerability Management
- CISA Cyber Resilience Review Supplemental Resource Guide Volume 3 Configuration and Change Management
- NIST Guide to Enterprise Patch Management Planning: Preventive Maintenance for Technology
- HHS HPH Sector Cybersecurity Framework Implementation Guide
- H-ISAC Vulnerability Management Cybersecurity for the Clinician Video Training
- 405d Prescription Poster: Vulnerability Management

Shifting Towards a More Secure Future: Secure by Design

With internet-facing systems connected to critical health systems and functions, it is crucial that manufacturers of technology products used by HPH entities employ secure by design practices. To that end, CISA co-authored and published Shifting the Balance of Cybersecurity Risk: Principles and Approaches for Secure by Design Software, which urges technology manufacturers to revamp their design and development programs to deliver products that have security built in and for which the default configuration is a secure one.

Historically, technology manufacturers and vendors have relied on one-off fixes for vulnerabilities after products have been deployed, requiring customers to apply patches at their own expense. CISA and its partners aim to shift the balance for product development to (1) secure-by-design, where the security of the customers is a core business requirement, not just a technical feature, and (2) secure-by-default, for product security out of the box, with no configuration changes needed and security features available without additional cost. Visit CISA's Secure by Design website for up-to-date guidance and information.

CISA recommends that manufacturers of HPH products take steps to build their products in a secure by design manner, and that HPH entities prioritize the importance of purchasing secure by design products. To do this, organizations should:

- **Develop and establish purchasing criteria that emphasizes the importance of secure by design practices.** Cybersecurity criteria should be incorporated into prospective procurements through vendor requests for information (RFIs).
  - For secure by design criteria, CISA recommends HPH entities look for manufacturers that follow secure by design principles. Examples include manufacturers that publish artifacts in line with CISA's secure by design guidance, such as publishing a secure by design and memory safety roadmap, providing Software Bill of Materials (SBOM), publishing a vulnerability disclosure policy, and documenting steps taken in accordance with NIST's Secure Software Development Framework (SSDF) and CISA's CPGs.
  - For secure-by-default configurations, HPH entities should look for products that eliminate default passwords, provide single sign-on (SSO) at no additional charge, include security audit logs at no additional cost, and integrate the most secure settings into the product by default.
- **Establish policies and procedures that require procurements of technology (including medical devices) undergo security evaluations.** Implementing cybersecurity evaluation provides an opportunity for your organization to understand, evaluate, and mitigate cyber risks prior to technology deployment. With the evaluation, HPH entities should insist on receiving a Manufacturer Disclosure Statement (MDS), which includes answers to questions such as:
  - Can this device display, transmit, or maintain private data (including electronic PHI/PII)?
  - Can the medical device create an audit trail?
  - Can users be assigned different privileged levels within an application based on 'roles' (e.g., guests, regular users, power users, administrators)?
- **Forge strategic partnership relationships with key IT suppliers.** Reinforce the importance of secure by design practices in both the formal contracts/vendor agreements and the informal aspects. Organizations should expect transparency from their technology suppliers.
  - When establishing formal contracts, HPH entities should require service level agreements (SLAs) and contracts with vendors and/or service providers that opt for more secure offerings, such as phishing-resistant MFA, the principle of least privilege for administrative accounts, auditing rights, and the disclosure and notification of confirmed security vulnerabilities within a risk-informed time frame.
- **Collaborate with industry peers.** Cultivate working relationships with industry partners to understand the products and services that best embody secure by design principles.

- **When leveraging cloud systems, ensure understanding of the supplier’s security responsibilities.** Organizations should prioritize cloud providers that are transparent about their security posture. Refer to CISA’s Secure Cloud Business Applications (SCuBA) Project for cloud security and configuration guidance.

HPH Sector Vulnerability Remediation Guidance

Upon implementing the mitigation strategies mentioned in the sections above, CISA encourages HPH Sector entities to track and prioritize their vulnerabilities based on their internal network architecture and risk posture.

Table 8 and table 9 show remediation guidance and compensating controls of the prioritized vulnerabilities identified sector wide, based on vulnerability scanning, high exploitation probability, top prevalence within the sector, and commercial risk rating categorizations.

Table 8: HPH Sector Prioritized Vulnerabilities

CVE	Vendor	Vulnerability Name
CVE-2021-44228	Apache	Apache Log4j2 Remote Code Execution Vulnerability
CVE-2019-11043	PHP	PHP FastCGI Process Manager (FPM) Buffer Overflow Vulnerability
CVE-2012-1823	PHP	PHP-CGI Query String Parameter Vulnerability
CVE-2021-34473	Microsoft	Microsoft Exchange Server Remote Code Execution Vulnerability
CVE-2017-12617	Apache	Apache Tomcat Remote Code Execution Vulnerability

Table 9: Prioritized Vulnerabilities Remediation and Mitigation Guidance

Remediation	Compensating Controls
CVE-2021-44228	
Upgrade to Log4j 2.17.1 (Java 8), 2.12.4 (Java 7) and 2.3.2 (Java 2).	• Disable Log4j library. Disabling software using the Log4j library is an effective measure, favoring controlled downtime over threat actor-caused issues. However, this option could cause operational impacts and limit visibility into other issues. • Disable Java Naming and Directory Interface (JNDI) lookups or disable remote codebases. This option, while effective, may involve developer work and could impact functionality. • Disconnect affected stacks. Solution stacks not connected to agency networks pose a dramatically lower risk from attack. Consider temporarily disconnecting the stack from agency networks. • Create a “vulnerable network” virtual local area network (VLAN) to isolate and segment the solution stack from the rest of the enterprise network. • Deploy a properly configured web application firewall (WAF) in front of the solution stack. • Consult CISA’s Apache Log4j Vulnerability Guidance webpage and GitHub repository for further updates and guidance.
CVE-2019-11043	
Upgrade to PHP version 7.3.11 or later.	• As Nginx is associated with this vulnerability, Nginx should be configured to check for existing scripts and files by including the `try_files` directive or using an if statement, such as `if (-f $uri)`. Note, this mitigation only works if Nginx and PHP-FRM share the same `docroot` on the same host. • Regularly patch and update PHP to its latest version and accordingly disable unnecessary or outdated plugins or components.

Remediation	Compensating Controls
	- Enable PHP's built-in security controls and use the Open Web Application Security Project (OWASP) PHP Configuration Cheat Sheet. - Implement validation and sanitation checks on all user-generated inputs or data. - Consider using address space layout randomization (ASLR). This technique increases the difficultly of performing a buffer overflow attack. ASLR randomly assigns the addresses of programs and functions in a system's memory to different data regions, making it difficult for a threat actor to navigate through sensitive functions in the memory.
CVE-2012-1823	
Upgrade to PHP version 5.3.12 / 5.4.2 or later.	- Use a `mod_rewrite` rule to direct the web server not to process requests with query strings beginning with a "`-`" and not containing a "`=`" through. - Regularly patch and update PHP to its latest version and disable unnecessary or outdated plugins or components. - Enable PHP's built-in security controls and use the Open Web Application Security Project (OWASP) PHP Configuration Cheat Sheet.
CVE-2021-34473	
Apply the most current vendor-issued security update and patches.	- To verify the current version of Microsoft Exchange running within an organization, reference Microsoft documentation regarding Exchange Server builds and releases. - Deploy a properly configured File Integrity Monitoring (FIM) solution to monitor and prevent creation of files. FIM solutions closely monitor both the configuration and content of sensitive files and trigger alerts whenever it comes across unauthorized access, copies, downloads, and modifications. - Implement a properly configured EDR solution to monitor access logs and help detect any deviations outside normal behavior. Ensure logs are securely stored and can only be accessed or modified by authorized and authenticated users. - Ensure MFA is in place for all external access, such as Outlook Web Access. - Disable remote PowerShell access for non-administrative users in the organization.
CVE-2017-12617	
Upgrade to Apache Tomcat version 9.0.1 or later.	- If you are a new user of Apache Tomcat, it is recommended to subscribe to the Apache Tomcat Mailing List to receive any information about new releases and security vulnerabilities. - The `readonly` `init-param` should be set to true, stopping a threat actor from uploading files. - Consider blocking `PUT` and `DELTE` requests on the frontend server (e.g., on the WAF).

Conclusion

This guide supports HPH entities by formulating recommendations based on pertinent malicious TTPs and vulnerability exposure data. As highlighted within this guide, HPH Sector entities should be vigilant in their vulnerability mitigation practices to prevent and minimize the risk from cyber threats. Once an organization assesses and deems a vulnerability a risk, it must treat the vulnerability.

CISA recommends HPH entities implement this guidance to significantly reduce their cybersecurity risk. CISA also strongly encourages HPH entities to use the threat intelligence information mentioned in the Cyber Risk Summary report[1] to effectively address and remediate their vulnerability exposure, and to protect their organizations from:

- Potential ransomware attacks,
- Data breaches,
- Loss or theft of equipment or data, and
- Attacks against network connected medical devices.

CISA also recommends HPH entities follow the mitigation strategies and recommendations addressed in this guide to improve organizational cybersecurity posture.

To further aid their organizations, CISA encourages HPH entities to sign up for CISA's free vulnerability scanning and welcomes HPH Sector entities to seek additional advice and assistance from CISA via vulnerability@cisa.dhs.gov.

Feedback regarding this product is critical to CISA's continuous improvement. If you have feedback specific to your experience with this product, please send CISA your input by filling out the CISA Product Survey.

Appendix #1 Glossary of Cyber Terms

Asset
The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.

Business Email Compromise (BEC)
A sophisticated scam that targets organizations and individuals by using social engineering or computer intrusion to compromise legitimate email accounts and conduct unauthorized fund transfer or obtain personally identifiable information.

Cybersecurity Risk
An effect of uncertainty on or within information and technology. Cybersecurity risks relate to the loss of confidentiality, integrity, or availability of information, data, or information (or control) systems and reflect the potential adverse impacts to organizational operations (i.e., mission, functions, image, or reputation) and assets, individuals, other organizations, and the Nation.

Information Technology (IT)
Any equipment or interconnected system or subsystem of equipment that processes, transmits, receives, or interchanges data or information.

Multifactor Authentication (MFA)
Multifactor authentication is a layered approach to securing data and applications where a system requires a user to present a combination of two or more credentials to verify a user's identity for login.

Operational Technology (OT)
Programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment).

Patch Management
The process of distributing and applying security updates to software and operating systems.

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

Security Configuration Management (SecCM)
The management and control of configurations for an information system to enable security and facilitate the management of risk.

Tactics, Techniques, and Procedures (TTPs)
The behavior of an actor. A tactic is the highest-level description of this behavior, while techniques give a more detailed description of behavior in the context of a tactic, and procedures an even lower-level, highly detailed description in the context of a technique.

Vulnerability
A characteristic or specific weakness that renders an organization or asset (such as information or an information system) open to exploitation by a given threat or susceptible to a given hazard.

Vulnerability Management
The process by which organizations identify, analyze, and manage vulnerabilities in a critical service's operating environment.

Appendix #2 Acronyms and Abbreviations

ACL – Access Control List

AES – Advanced Encryption Standard

API – Application Programming Interface

ASLR – Address Space Layout Randomization

ATT&CK – Adversarial Tactics, Techniques, and Common Knowledge

BEC – Business Email Compromise

CCM – Configuration and Change Management

CISA – Cybersecurity and Infrastructure Security Agency

CPG – Cybersecurity Performance Goal

CPU – Central Processing Unit

CRS – Cyber Risk Summary

CSA – Cybersecurity Advisory

CVSS – Common Vulnerability Scoring System

CyHy – Cyber Hygiene

CY – Calendar Year

EDR – Endpoint Detection and Response

ePHI – Electronic Protected Health Information

EPSS – Exploit Prediction Scoring System

ECDSA – Elliptic Curve Digital Signature Algorithm

FBI – Federal Bureau of Investigation

FIM – File Integrity Monitoring

FTP – File Transfer Protocol

HHS – U.S. Department of Health and Human Services

H-ISAC – Health Information Sharing and Analysis Center

HIPAA – Health Insurance Portability and Accountability Act

HPH – Healthcare and Public Health

HSM – Hardware Security Module

IDS – Intrusion Detection System

IT – Information Technology

JNDI – Java Naming and Directory Interface

KEV – Known Exploited Vulnerability

LDAP – Lightweight Directory Access Protocol

MFA – Multifactor Authentication

MDS – Manufacturer Disclosure Statement

NetBIOS – Network Basic Input/Output System

NIST – National Institute of Standards and Technology

OS – Operating System

OT – Operational Technology

OWASP – Open Web Application Security Project

PHI – Protected Health Information

PII – Personally Identifiable Information

PKI – Public Key Infrastructure

RDP – Remote Desktop Protocol

RFI – Request for Information

RPC – Remote Procedure Call

SBOM – Software Bill of Materials

SecCM – Security Configuration Management

SIEM – Security Information and Event Management

SMB – Server Message Block

SMS – Short Message/Messaging Service

SNMP – Simple Network Management Protocol

SOP – Standard Operating Procedure

SPF – Sender Policy Framework

SQL – Structured Query Language

SSO – Single Sign-On

SSVC – Stakeholder-Specific Vulnerability Categorization

TCP – Transmission Control Protocol

Telnet – Teletype Network

TLS – Transport Layer Security

TTP – Tactics, Techniques and Procedures

UEBA – User and Entity Behavior Analytics

VLAN – Virtual Local Area Network

VPN – Virtual Private Network

VS – Vulnerability Scanning

WAF – Web Application Firewall

WAS – Web Application Scanning

WebAuthn – Web Authentication