Cybersecurity Performance Goals Adoption Report

Publication: 2024
Cybersecurity and Infrastructure Security Agency

Table of Contents

Summary 3
Background 3
Cyber Hygiene Enrollment 5
CPG Adoption Analysis 6
1.E: Mitigating Known Vulnerabilities 6
2.K: Strong and Agile Encryption 8
2.M: Email Security 10
2.W: No Exploitable Services on the Internet 10
2.X: Limit OT Connections on the Public Internet 13
4.C: Security.txt Adoption 15
Conclusion 16
Appendix 17

SUMMARY

The Cybersecurity and Infrastructure Security Agency (CISA) defines Cross-Sector Cybersecurity Performance Goals (CPGs) as a subset of cybersecurity practices selected through a thorough process of industry, government, and expert consultation aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. Although CPGs are voluntary in nature, they aim to help organizations develop and enhance their investment in cybersecurity efforts. CISA's CPGs have been organized to align to the National Institute of Standards and Technology's (NIST's) Cybersecurity Framework 1.0 (CSF 1.0)'s five main functions: identify, protect, detect, respond and recover. CISA's initiatives and programs are driving service enrollments and CPG adoption across critical infrastructure sectors with the strongest impact seen in Healthcare and Public Health, Water and Wastewater Systems, Communications, and Government Services and Facilities sectors.

Key Findings:

- Exploitable services routinely monitored by CISA Vulnerability Scanning have been steadily decreasing from 12 services per enrollee in August 2022 to about eight services per enrollee in August 2024 **(Figure 13).**
- Across the period of analysis, remediation times for Secure Sockets Layer (SSL) vulnerability and known exploited vulnerability (KEV) tickets decreased by 50% for critical-severity KEVs and by 25% for high-severity KEVs **(Figures 4 and 5).**
- In August 2022, SSL vulnerability-related tickets were resolved in about 200 days. During the later months, resolution time decreased to under 50 days **(Figure 7).**
- As of Aug. 31, 2024, CISA observed the highest occurrence of operation technology (OT) protocols exposed to the public internet within the Government Services and Facilities sector at 63% exposure **(Table 2).**

Organizations should remain up to date on cybersecurity hygiene and best practices to protect against adversary threats related to gaps in network infrastructure. Internet-facing exposed services and assets should remain a priority for remediation in conjunction with the above key findings. CISA also encourages sector entities to review NIST Special Publication (SP) 800-53 Rev. 5, Security and Privacy Controls for Information Systems and Organizations and the NIST Cybersecurity Framework for additional best practices.

BACKGROUND

This report assesses the inferred adoption of select CISA CPGs since the report's initial release on October 27, 2022, and update on March 21, 2023. Analysis focuses on six CPGs and is based on vulnerability exposure across 7,791 critical infrastructure organizations enrolled in CISA's Vulnerability Scanning service from Aug. 1, 2022, through Aug. 31, 2024. The six CPGs included in this report are 1.E: Mitigating Known Vulnerabilities; 2.W: No Exploitable Services on the Internet; 2.K: Strong and Agile Encryption; 2.X: Limit OT Connections on the Public Internet; 4.C: Deploy a Security.txt file; and 2.M: Email Security.

In several of the metrics calculations, ratios are used along the vertical axes of the graphics. As the number of enrollees grows over time, the volume of their associated metrics (e.g., vulnerabilities, configuration statuses, or security incidents) will naturally increase. To accurately convey trends and performance over time, it is important to contextualize these raw counts relative to the size of the population being measured. Using ratios (e.g., metric counts per enrollee) enables data normalization and accounts for enrollee population fluctuations.

CYBER HYGIENE ENROLLMENT

Over the period of analysis, the total Cyber Hygiene (CyHy) service enrollment increased by 201% **(Figure 1)**. This increase is likely a result of CISA programs and initiatives, such as the CPGs, targeted risk analysis and intel products, and other efforts. All sectors exhibited an average of 208% growth in enrollment since CPG publication. The sectors that showed the highest enrollment increase were the Communications (300%), Emergency Services (268%), Critical Manufacturing (243%), and Water and Wastewater Systems (242%) sectors.

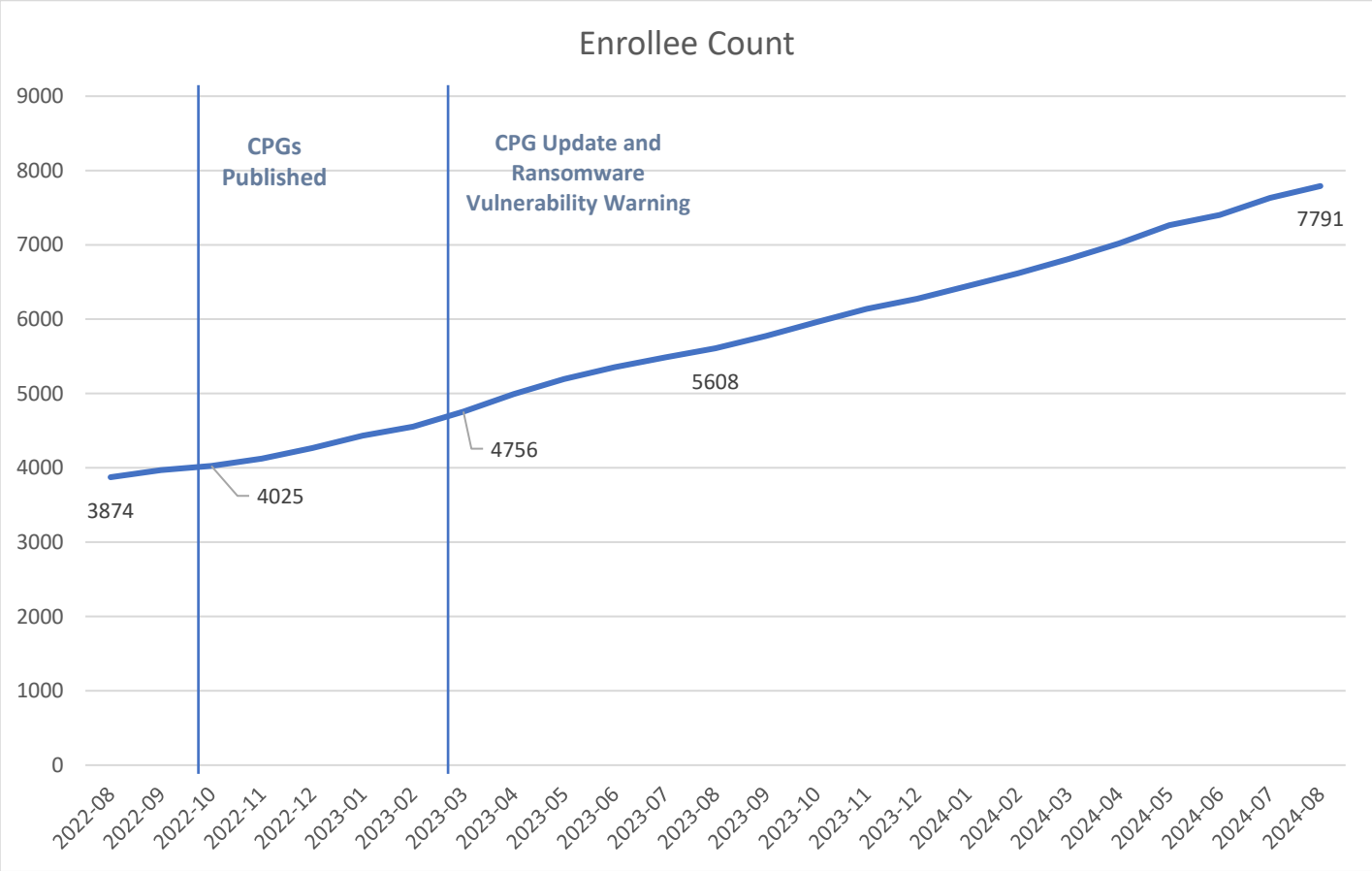


Figure 1: Total CyHy Enrollments Count

CPG ADOPTION ANALYSIS

1.E: Mitigating Known Vulnerabilities

As of Aug.31, 2024, CISA's Known Exploited Vulnerabilities (KEV) Catalog recorded a total of 1,199 KEVs. Enrolled organizations continue to demonstrate progress in mitigating KEVs on their internet-accessible assets.

Since publication of the CISA CPGs, entities enrolled in CISA's Vulnerability Scanning service demonstrated a continued decline in the average number of KEVs on their networks. This indicates that critical infrastructure organizations are successfully prioritizing the remediation of vulnerabilities based upon KEVs.

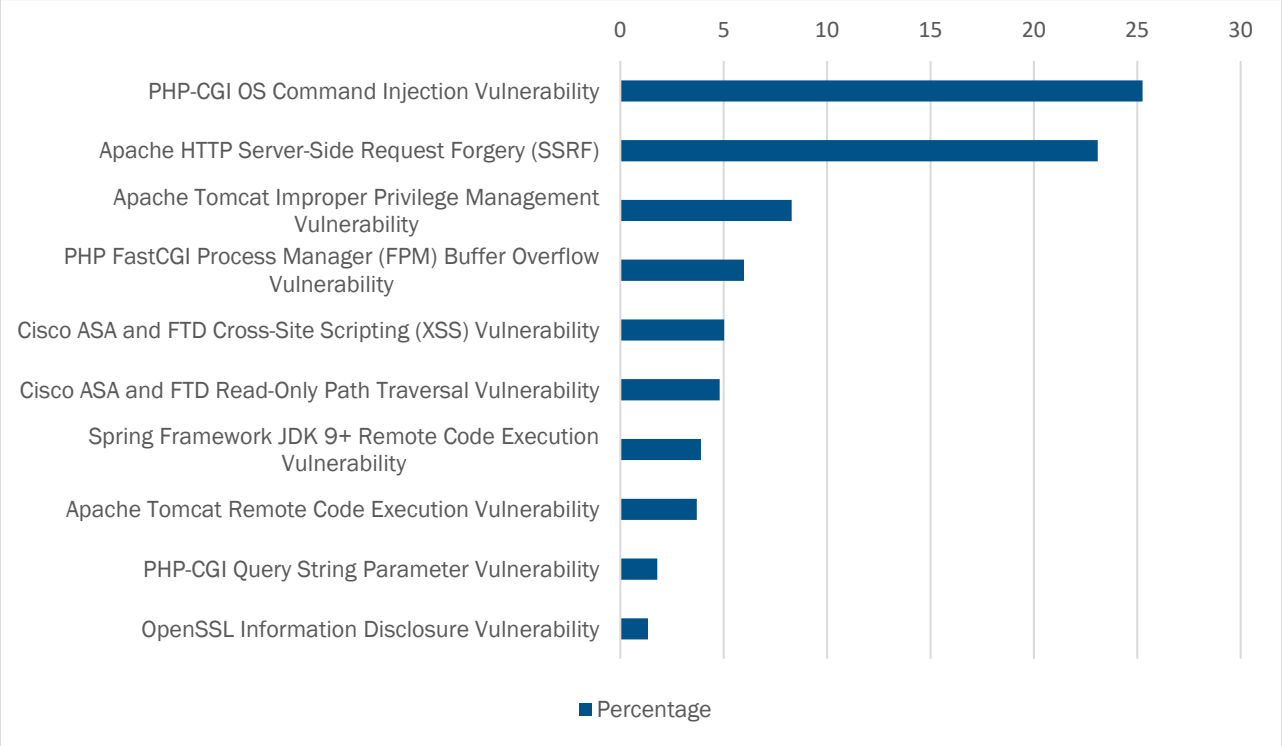


Figure 2: Top 10 Observed KEVs

Data on the top 10 KEVs over the review period reveals notable trends in the cybersecurity landscape for CyHy enrollees. A significant portion of the vulnerabilities involved open-source software, with PHP and Apache-related vulnerabilities collectively accounting for over half of the cases (58%). This includes high-prevalence KEVs such as PHP-CGI OS Command Injection Vulnerability (25.3%) and Apache HTTP Server-Side Request Forgery (23.1%), highlighting the widespread use and potential risks in these platforms. Cisco-related vulnerabilities, though less frequent, represent 9.8% of observed KEVs.

The recurrence of vendors like PHP, Apache, and Cisco indicates that vulnerabilities in popular and widely used software platforms continue to be a critical challenge for CyHy enrollees. This data underscores the importance of targeted mitigation strategies focused on the most exploited platforms **(Figure 2).**

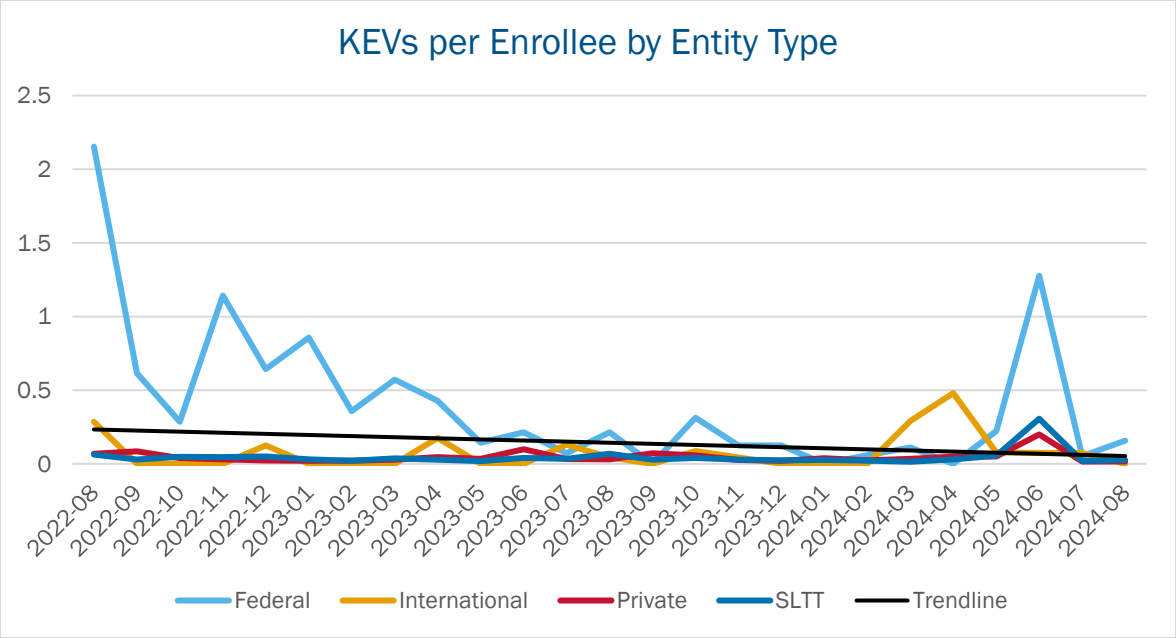
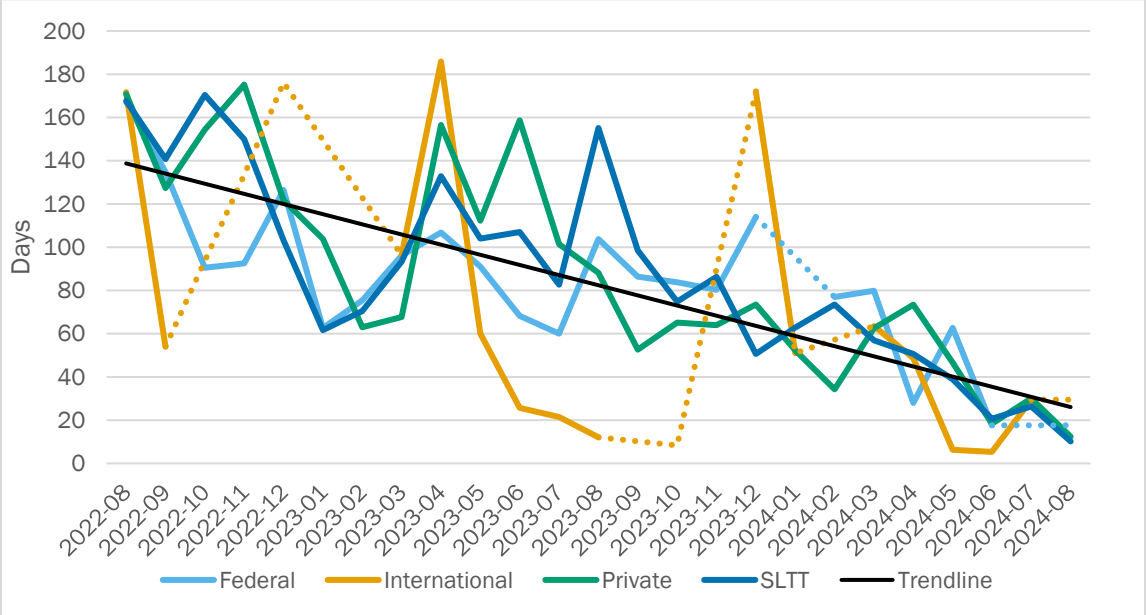


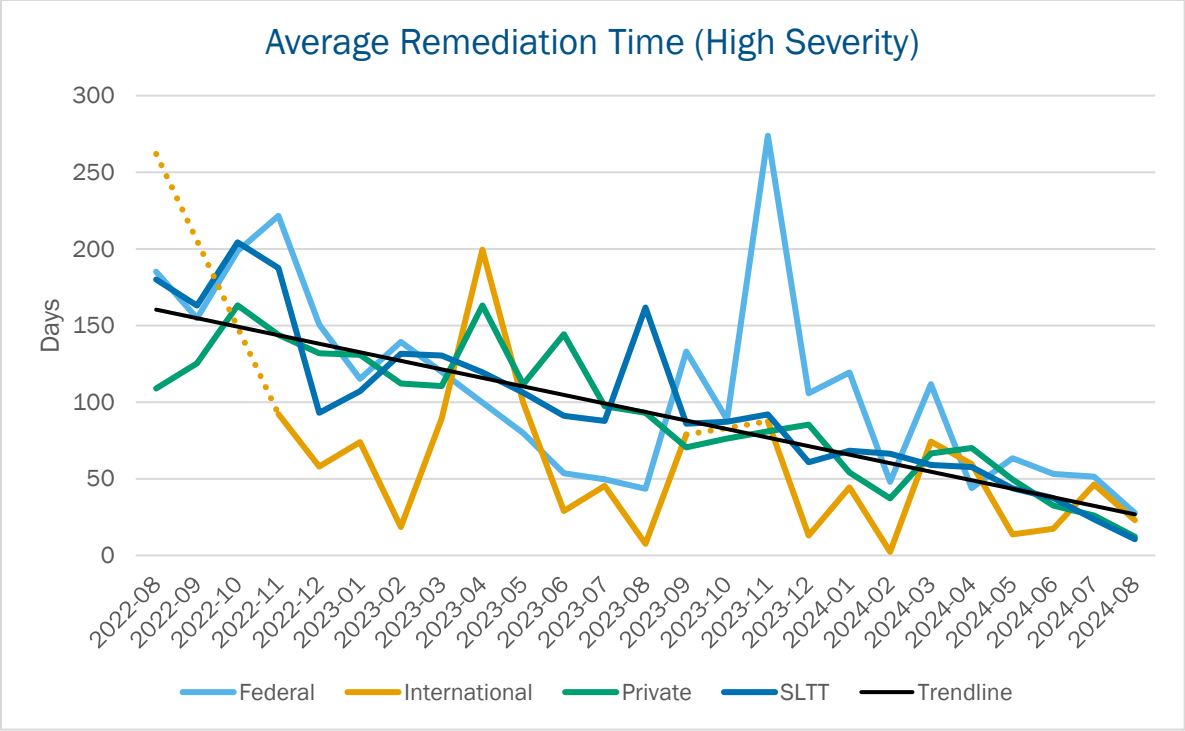
Figure 3: Average KEVs per CyHy Enrollee by Entity Type

During the period of analysis, most entities displayed an average KEV rate below 0.5. Additionally, the most recent reporting period trendline shows an overall reduction in total KEVs per entity based on CyHy enrollee ticket data between August 2022 and August 2024 **(Figure 3).**



Note: Dotted lines represent gaps in collection that were interpolated for clarity.
Figure 4: Average Remediation Time of Critical Severity KEVs

Average remediation time for high and critical vulnerabilities were reduced during the reporting period of August 2022 through August 2024. Based on the most recent six-month period between February 2024 and August 2024, the trendline shows average remediation times have been reduced from 60 days to 30 days and by 50% for critical vulnerabilities and by 25% for high vulnerabilities **(Figures 4 and 5).**



Note: Dotted lines represent gaps in collection that were interpolated for clarity.

Figure 5: Average Remediation Time of High-Severity KEVs

2.K: Strong and Agile Encryption

Out-of-date encryption protocol configurations increase the likelihood of sensitive and valuable data exposure to adversaries. CISA observed multiple outdated encryption instances of SSL version 2 and 3, Transport Layer Security (TLS) version 1.0, and TLS version 1.1 across all critical infrastructure sectors. Prior to the CPG publication, increased outdated encryption protocol instances were observed across critical infrastructure sectors. **Figure 6** shows the SSL misconfiguration vulnerability count per cumulative enrollees on a month-to-month basis. The first 11 months of data (August 2022 to July 2023; note that two outliers were removed) showed the average ratio of misconfiguration was 3.8, while the last 12 months (August 2023 to August 2024) showed a decrease to 2.5 vulnerability count per enrollee.

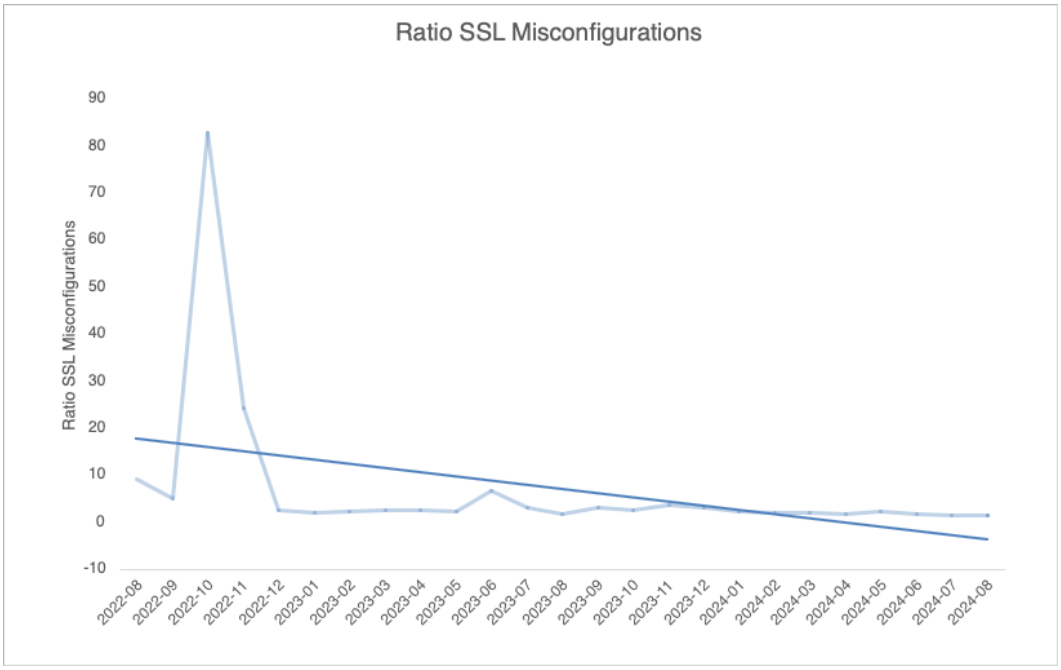


Figure 6: Ratio of SSL Misconfigurations

The average time to resolve all SSL findings is illustrated in **Figure 7**. In August 2022, the initial remediation time was 197 days. This time significantly decreased to 12 days as of August 2024. This is an average of eight days reduction in time to remediate on a month-to-month basis. In addition, SSL misconfiguration findings were 45% of the total findings of all vulnerabilities detected, on average, on a month-to-month basis. SSL misconfiguration findings were 50% or more of the vulnerabilities detected for 17 of the 25 months analyzed (August 2022 to August 2024). However, from March to August 2024, SSL misconfiguration vulnerabilities decreased to an average of 33.5% from 63% of total vulnerabilities reported.

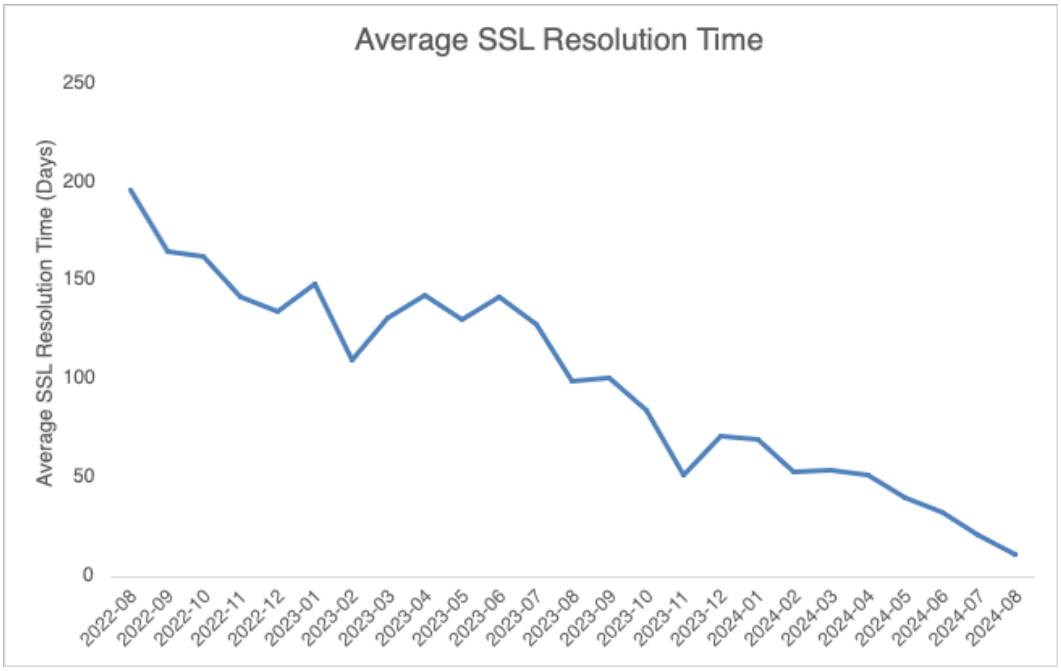


Figure 7: Average SSL Resolution Time

2.M: Email Security

CISA assessed email security configurations of all CyHy enrollees by checking for prevention against email spoofing and validating email authenticity. The three configurations that provide the strongest email security are Domain-based Message Authentication, Reporting, and Conformance (DMARC), Sender Policy Framework (SPF), and STARTTLS (opportunistic Transport Layer Security). CISA's best practices recommend that organizations configure all three mechanisms to achieve optimal email security and combat malicious activity. While almost all CyHy enrollees demonstrated partial implementation of at least one of these security options, DMARC was the most implemented with a configuration percentage of 89%. A configuration of DMARC and SPF together totaled 7%. Implementation of all three configurations was 2%. **Figure 8** provides a breakdown of email security protocols adopted across all CyHy enrollees.

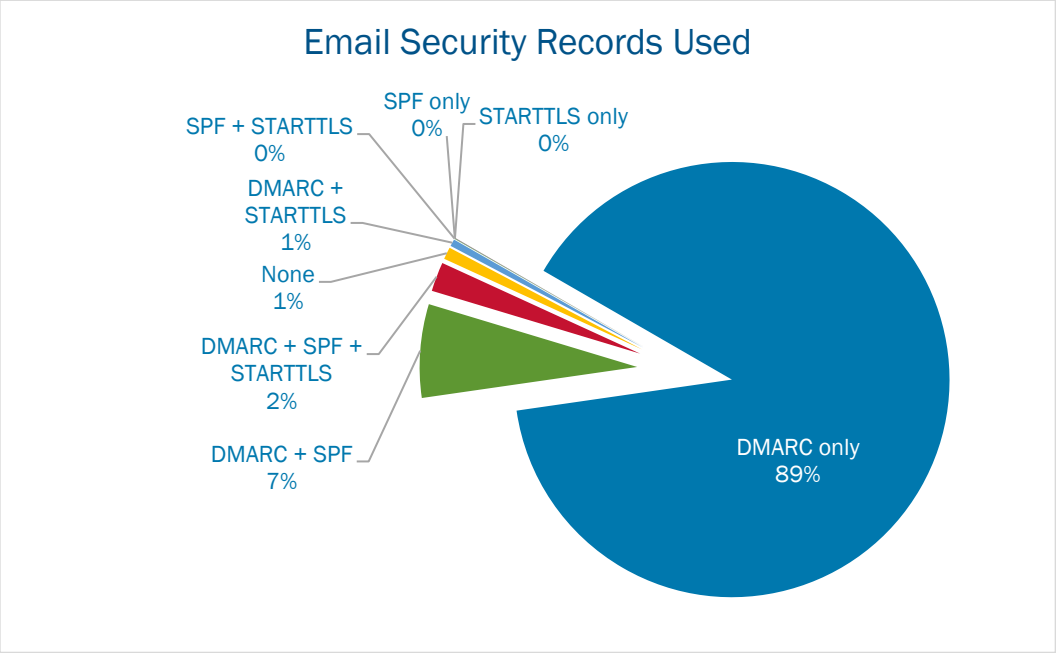


Figure 8: Email Security Record Breakdown

2.W: No Exploitable Services on the Internet

As of Aug. 31, 2024, roughly 83% of CyHy stakeholders originally observed at the beginning of the period of analysis (Aug. 1, 2022) all instances of their exploitable services had been remediated **(Figure 9)**.

CISA scans for potentially exploitable services that can increase an entity's risk of exposure **(see Appendix)**. Although occasional month-to-month increases were recorded, over the entire period of analysis and post-CPG publications, CISA observed positive trends toward the reduction of exploitable services on the internet amongst various sectors of enrolled organizations **(Figures 10 and 11)**.

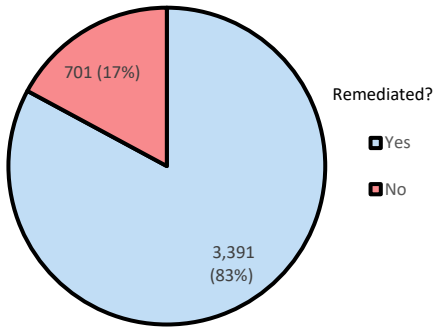


Figure 9: Total Remediation of Exploitable Services

Figure 10 corresponds to the total exploitable service instances amongst federal and international stakeholders within the period of analysis. Federal organizations experienced a decline of roughly 60% in the number of exploitable service instances over the entire period of performance. Similarly, international entities experienced a 65% decrease over the same period.

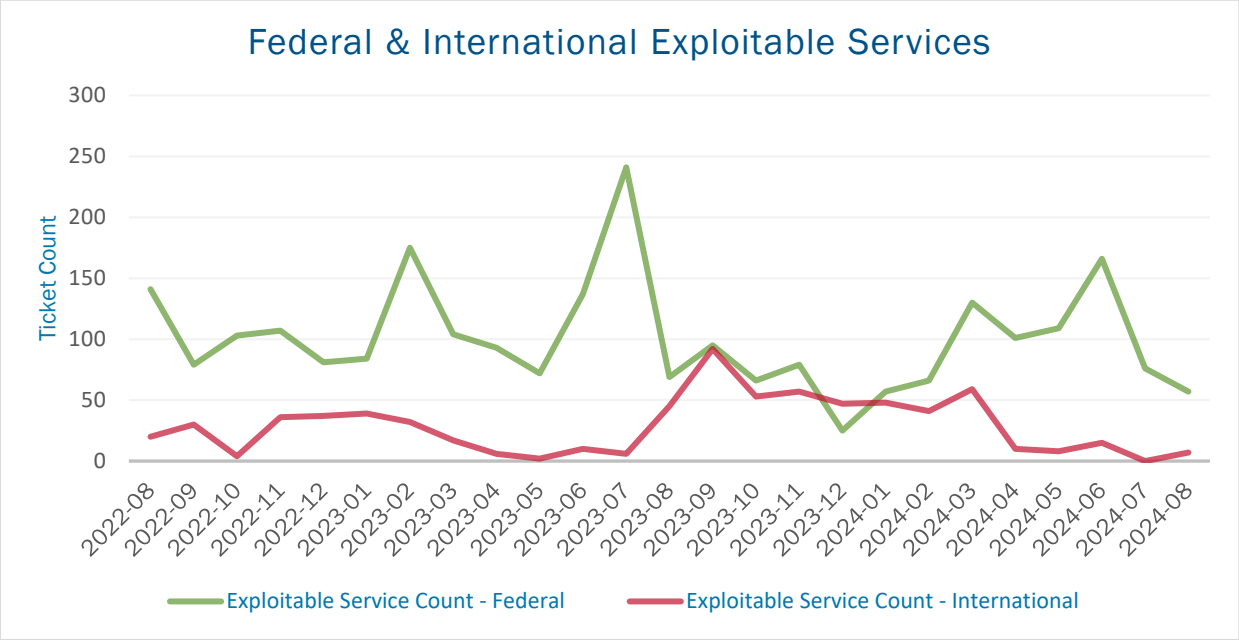


Figure 10: Exploitable Federal and International Services

Figure 11 corresponds to the total exploitable service instances amongst state, local, tribal, and territorial (SLTT) entities as well as private entities. Although SLTT entities observed a 61% decrease in exploitable service instances between October 2022 and April 2023, the number of instances observed amongst SLTT organizations increased by roughly 95% over the entire period of analysis. In contrast, private entities observed a consistent downward trend that equated to a 79% decrease in exploitable service instances within the period of analysis.

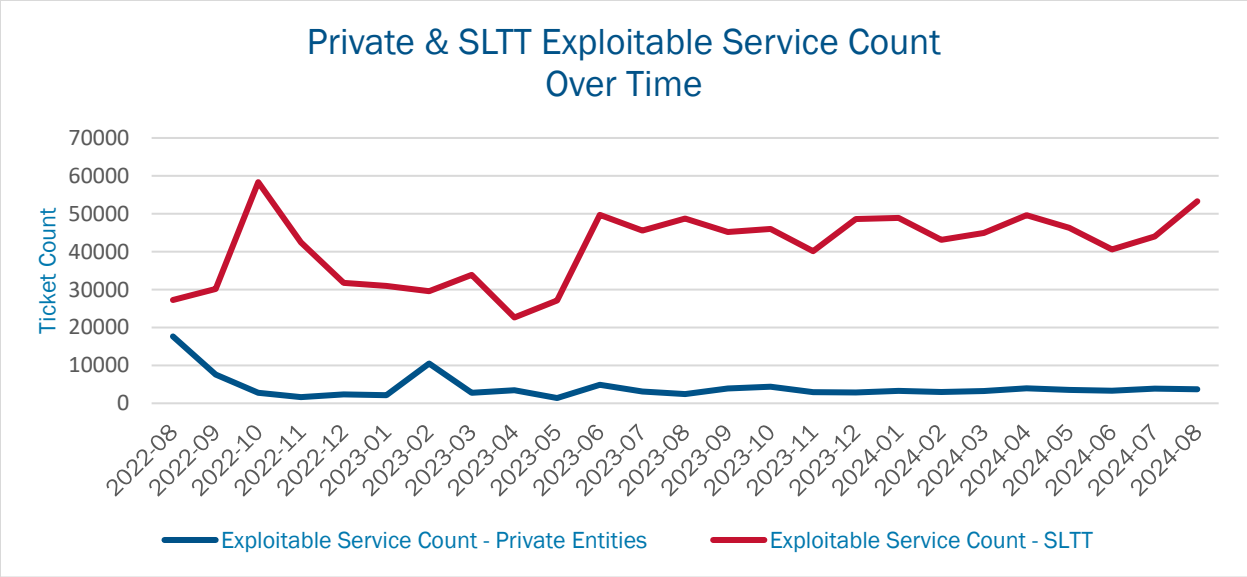


Figure 11: Exploitable Services of Private and SLTT Entities

Progress has been made to reduce exposure of exploitable services across most of the critical infrastructure sectors month over month within the period of analysis between Aug. 1, 2022, to Aug. 31, 2024. The top five exploitable services and the total count remaining are shown with the most exposure across all critical infrastructure sectors, including File Transfer Protocol (FTP), Remote Desktop Protocol (RDP), Remote Procedure Call (RPC), Server Message Block (SMB), and Internet Relay Chat (IRC). The remaining exploitable services are labeled as “other services” in **Figure 12**.

Three exploitable services illustrated a decrease in ticket instances among entities observed over the entire period of analysis. Of these three, SMB experienced the most drastic decrease of roughly 72% from August 2022 to August 2024. In contrast, the other two services, IRC and RPC, experienced increases in ticket instances observed over the same period. Although RPC accounted for roughly 92% of all exploitable service ticket instances **(Figure 12),** the vulnerable RPC ratio was observed to decrease from 9.5 tickets per entity in August 2022 to just over 6.5 tickets per entity in August 2024.

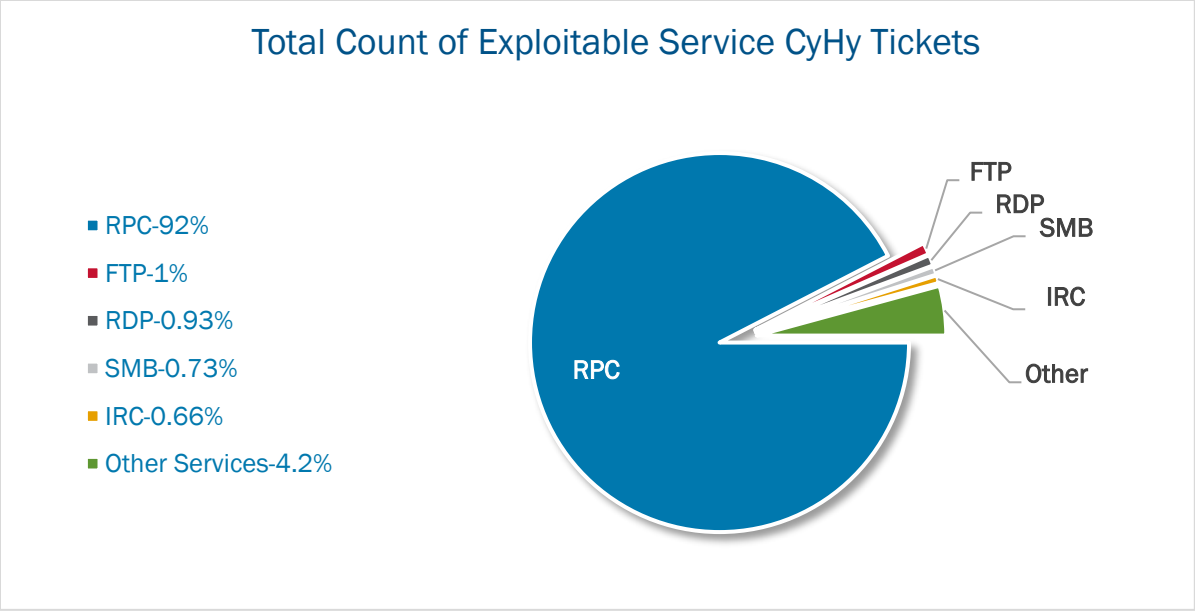


Figure 12: Exploitable Service Breakdown

Figure 13 illustrates all exploitable services combined into a ratio to show their prevalence per month. It also shows the enrollee ratio during the same period, exemplifying the decline in exploitable services' totality. Periods where there were increases in exposure most likely correlate to an expansion of assets scanned because of increased CyHy customer enrollment. CISA continuously promotes vulnerability management and reduction services to increase CyHy enrollment and gain better visibility into internet-facing assets.

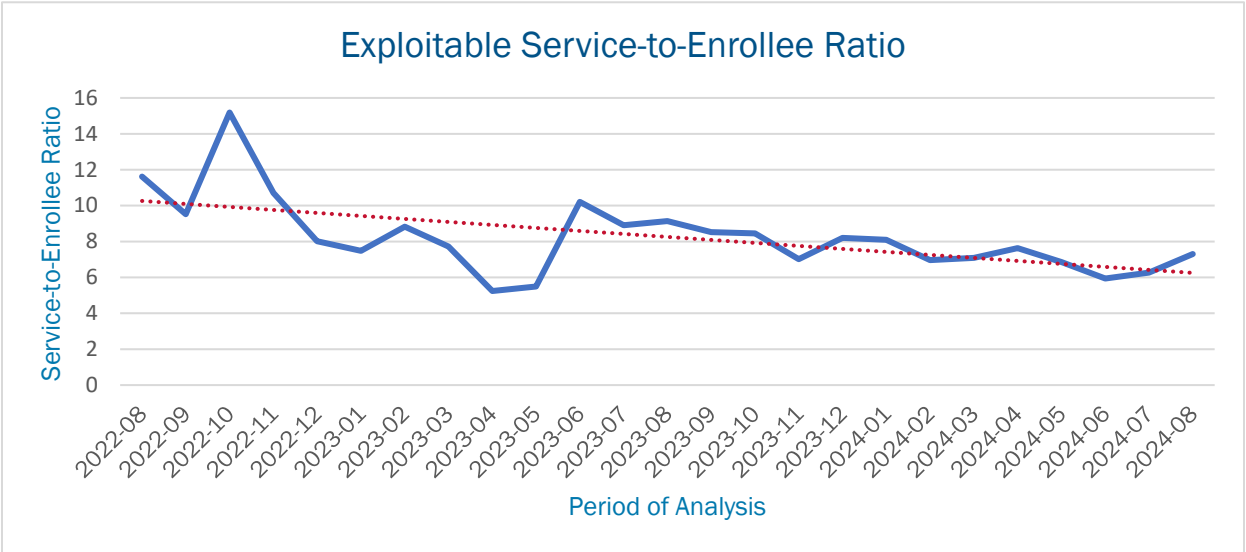


Figure 13: Exploitable Services and Enrollee Ratios

2.X: Limit OT Connections on the Public Internet

CISA identified the top OT/Industrial Control Systems (ICS) protocols commonly used with OT/ICS products **(Table 1)** exposed to the public internet. CISA port scans have only been available for the past 90–150 days; therefore, CISA is not able to determine OT/ICS exposure prior to CPG publication. As of Aug. 31, 2024, CISA observed the highest occurrence of OT protocols exposed to the public internet and observed the top five publicly exposed OT/ICS protocols from Oct. 11, 2023, to Aug. 31, 2024. Port scans do not reveal specific ICS devices associated with these protocols; however, these are common protocols associated with OT connections that are being exposed to the public internet.

Table 1: Common OT/ICS Protocols

Protocol	Associated Ports
Open Platform Communications Unified Architecture (OPC UA)	4840 (TCP), 4843 (TCP)
Distributed Network Protocol (DNP)	20000 (TCP/UDP), 19999 (UDP)
Niagara-Fox	1911 (TCP), 4911 (TCP)
Ethernet/IP	2222 (UDP), 44818 (TCP)
Modbus (MBAP)	502-507 (TCP), 802 (TCP), 1051 (TCP), 4001 (TCP), 5000 (TCP), 5252 (TCP)

As of September 2024, CISA observed OT protocols exposed to the public internet and determined five sectors with the highest occurrences **(Table 2)**. Exposure of the most observed OT/ICS protocols **(Table 1)** across most of the critical infrastructure sectors was observed, as well as the percentage of findings from CyHy enrollees **(Figure 14)** from Oct. 11, 2023, to Aug. 31, 2024. The Government Services and Facilities sector primarily exposes the OPC UA protocol which is widely used within ICSs.

Table 2: OT/ICS Protocol Exposure per Critical Infrastructure Sector

Critical Infrastructure Sector	Percentage Exposed
Government Facilities	63%
Information Technology	10%
Energy	10%
Healthcare and Public Health	5%
Financial Services	4%

Figure 14 displays the percentage of discovered exposed OT/ICS devices enrolled in CISA's CyHy program.

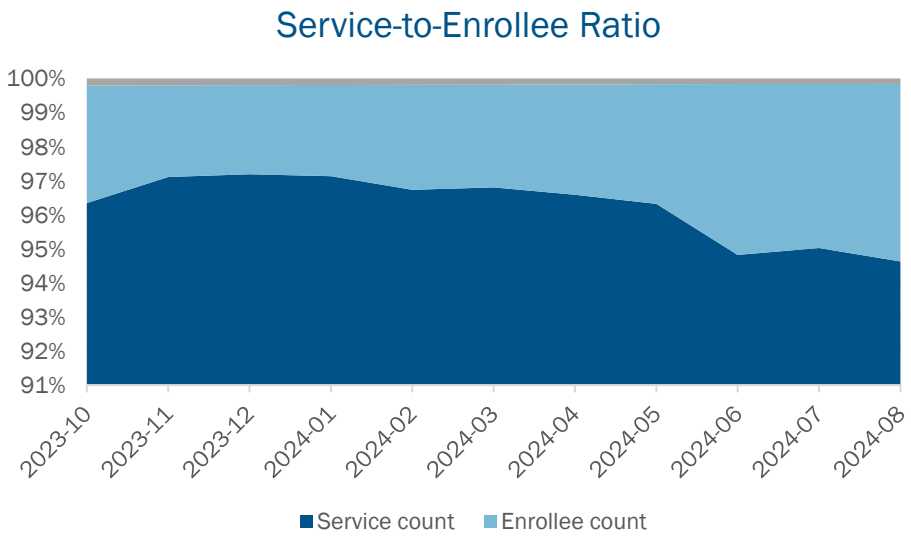


Figure 14: Ratio of CyHy Enrollees Observed with OT Protocols Exposed to the Public Internet

Figure 15 identifies the most observed OT/ICS protocols exposed to the public internet during the period of analysis.

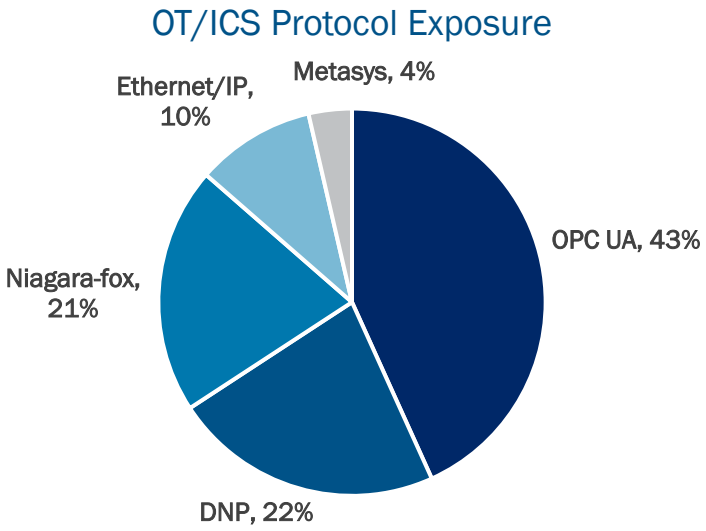


Figure 15: Common OT Protocols Exposed to the Public Internet

4.C: Security.txt Adoption

In September 2020, CISA published a binding operational directive requiring federal agencies to develop and publish a vulnerability disclosure policy. The security.txt file is one of the proposed standards to satisfy this directive. While many CyHy enrollees demonstrated partial implementation of the security.txt configuration with only point-of-contact information filled in, full implementation of the security.txt file is slow. Less than one percent of the top one million sites on the internet are utilizing it as of late 2022.[1,2] Some cloud providers are offering to generate the security.txt file for their customers; this feature would generate a compliant security.txt file for immediate use. RFC 9116 outlines that the security.txt file must be hosted on an encrypted HTTP service, which predominantly is port 443. Port 8443 also supports the encryption that port 443 uses and is less known. Ports 80 and 8080 are not safe as they are originally plain text and are not to host the security.txt file in that state. However, port 8080 can be configured manually to support the necessary encryption. The graph below represents the prevalence of federal civilian executive branch (FCEB) service ports hosting the security.txt file.

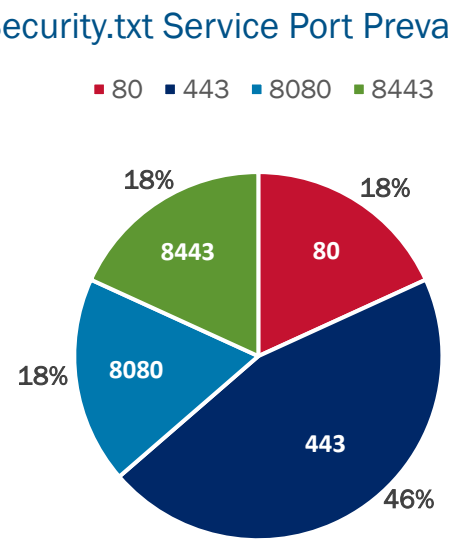


Figure 16: Cloud Hosting Security.txt File Exposure per Service Port

As organizations migrate more data to cloud environments, preventing unauthorized access to both the data and the connected network becomes crucial. A key component in managing cyber threats is the ability to reference, parse, and communicate exploitation events through a properly formatted and hosted security.txt file. Adoption of the security.txt file within critical infrastructure sectors in the U.S. has grown alongside increased cloud usage. A well-crafted service-level agreement (SLA) is crucial to understand the responsibilities of the organization and of the cloud provider.

[1] Naz Markuta, "1 Million Websites - How Many Use Security.txt?" Hexiosec, October 26, 2022, https://redmaple.tech/blogs/2022/survey-of-security-txt/#bonus-moz-top-500.
[2] William P. Findlay and AbdelRahman Abdou, "Characterizing the Adoption of Security.txt Files and Their Applications to Vulnerability Notification," n.d., https://people.scs.carleton.ca/~abdou/findlay2022_madweb_authors_copy.pdf.

The cloud introduces many challenges with the ability to spin up multiple devices available to the internet with relative ease and by offering operating systems that have surpassed their end-of service date. Over 7,400 common vulnerabilities and exposures (CVEs) were observed on vulnerable cloud systems hosting the security.txt file from insecure versions exposed to the internet as of September 2024. These vulnerable systems could serve as a malicious pivot point to an organization's sensitive network segments. Table 3 displays the prevalence of the top five OSs hosting the security.txt file externally facing from a cloud platform.

Table 3: Cloud Hosting Security.txt File Exposure per OS

OS Hosting Security.txt	Prevalence Exposed
Ubuntu	60%
Windows NT 6.2 and above	35%
Windows NT 6.0 and below	3%
Windows 7 (NT 6.1)	1%
Synology DiskStation	1%

For these reasons, organizations must understand the sensitivity of the data they store in the cloud and select the appropriate security controls to properly protect their data. Organizations must also make the security.txt file accessible in a compliant manner in accordance with RFC 9116. Proper configuration of the security.txt file will foster effective and timely communication channels for vulnerabilities to be researched and reported to strengthen reaction time to cyberattacks and counter zero-day vulnerabilities. For more information concerning cloud security, refer to CISA and NSA joint publications.[3]

CONCLUSION

Overall, CISA initiatives, programs, and products are directly influencing critical infrastructure sector service enrollments and adoption of CPGs. General analysis of CISA data reveals a moderate impact of CPG adoption across critical infrastructure sectors. This is most evident in the Healthcare and Public Health, Water and Wastewater Systems, Communications, and Government Services and Facilities sectors where there appears to be strong partnership and collaboration with CISA. As CISA strengthens partnerships across all sectors, CPG adoption will continue to expand. Additionally, as CISA continues to evolve CPG guidance, CPG adoption analytics will be more granular and apparent. Over time, this advancement will allow CISA to infer adoption of more CPGs.

[3] "CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices," CISA, March 7, 2024. https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices.

APPENDIX

Service	Description
FTP	File Transfer Protocol (FTP) is used for the transfer of files between a client and server on a network over a cleartext or unencrypted protocol. Cleartext passwords used for authentication are susceptible to sniffing, spoofing, and brute force attacks that can lead to data loss and unauthorized internal network access.
IRC	Internet Relay Chat (IRC) is an unencrypted protocol that facilitates communication in the form of text for group communication. Threat actors may be able to gather sensitive information from IRC communications between users and launch denial-of-service attacks on IRC traffic to disrupt user-to-user interaction.
Kerberos	Kerberos is a computer-network authentication protocol that facilitates communication over a non-secure network in a more secure manner. An unpatched Kerberos connection may allow a threat actor to authenticate onto an entity's network and conduct malicious activity under a legitimate guise.
LDAP	Lightweight Directory Access Protocol (LDAP) is an application protocol that allows clients to perform a variety of operations in a directory server. When exposed to the internet, LDAP could be used by threat actors to gather and manipulate sensitive information related to users, systems, services, and applications on a network.
NetBIOS	Network Basic Input/Output System (NetBIOS) is an unauthenticated protocol that allows applications on computers to communicate over a local area network. When NetBIOS is exposed to the internet, threat actors may be able to reach directories and files and gather sensitive information from devices communicating over the network.
RDP	Remote Desktop Protocol (RDP) allows remote connection to a computer over a network, which can be exploited when misconfigured. RDP should be kept internal to an organization's network and multifactor authentication (MFA) should be used to secure access. Threat actors can use RDP to facilitate data theft and exposure, hijacking of login credentials, and installation of malware and ransomware.
RPC	Remote Procedure Call (RPC) enables data exchange and functionality from a different location on the computer, network, or across the internet. Leaving RPC open to the internet may enable threat actors to penetrate the defensive perimeter, exfiltrate data, and modify configurations.
SMB	Server Message Blocks (SMB) is a protocol that provides shared access to files, printers, and serial ports between nodes on a network. SMB lacks support for secure authentication protocols.
SQL	Standard Query Language (SQL) is a standard computer language for managing data held in a relational database and used to query, insert, update, and modify data. Insecure implementations of SQL can be leveraged by threat actors to retrieve sensitive data on database interfaces.
Telnet	Teletype Network (Telnet) is an application protocol used on the internet or local area network for unencrypted text communications that poses a severe security risk when exposed to the internet. Threat actors can see and manipulate the traffic to and from devices with ease.