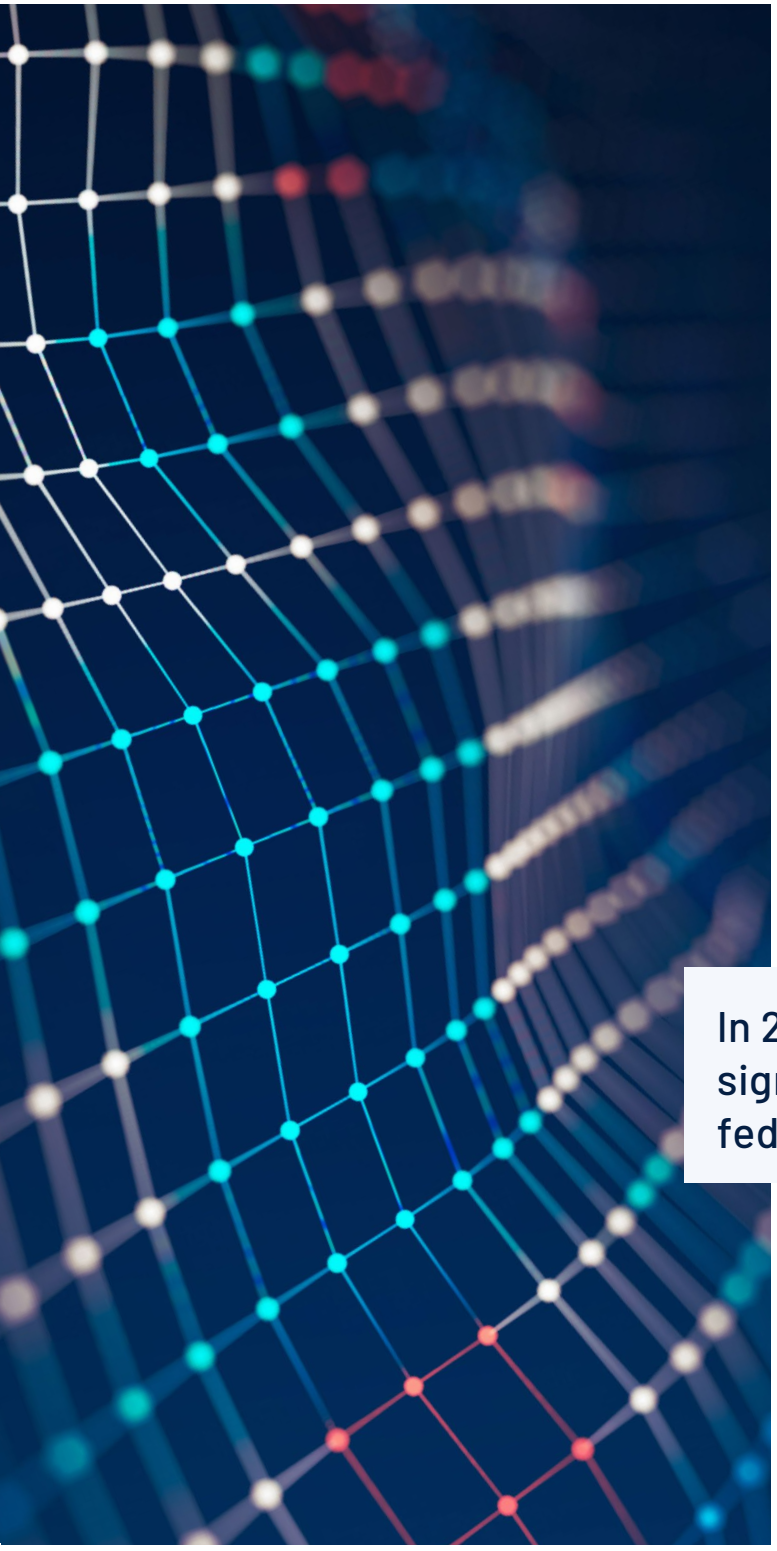
tenable

TENABLE FEDERAL EBOOK

PROTECTING FEDERAL GOVERNMENT INFRASTRUCTURE AND DATA FROM CYBER ATTACKS



Cybersecurity professionals at government agencies face many of the same challenges, and share many of the same needs, as their commercial counterparts. However, public sector security teams must often deal with complicating factors that make their jobs especially difficult. Those factors, including strict compliance mandates, budget uncertainties, staff shortages, skill gaps and more- arguably place government cybersecurity challenges in a class of their own.

To make matters worse, for many attackers, government agencies are an especially attractive target given the mass amount of sensitive data they possess, ranging from personal information about citizens to classified information pertaining to national security. Add to that the sophistication and frequency of cyber attacks continue to increase exponentially, posing a significant risk to individual and national security.

In 2022 alone, there were more than 140 significant cybersecurity events against federal agencies and their partners.[1]

Recognizing the critical importance of security amid this threat landscape, the Biden Administration issued Executive Order 14028, "Improving the Nation's Cybersecurity," in May 2021.[2] This legislation requires federal agencies to examine their attack surfaces and adopt a Zero Trust security model. This model aims to limit potential attack surfaces by restricting access to sensitive data and systems to users with proper authorization, and continuously verifying their permissions. This model also treats all network traffic as potentially malicious and requires additional layers of security.

Strategies to secure federal systems and data

To meet the requirements of EO 14028, federal agencies need to implement best-in-class exposure management. Tenable helps further the federal government's mission by protecting sensitive information, maintaining public safety, reducing financial risk, and ensuring compliance. With this in mind, Tenable has developed five strategies that agencies can use to protect their infrastructures and data from cyber attacks:

1. **Invest in risk-based vulnerability management (VM)**
2. **Safeguard critical infrastructure**
3. **Implement a Zero Trust strategy**
4. **Secure Active Directory (AD)**
5. **Leverage cloud solutions that achieve FedRAMP compliance**

These strategies will assist agencies in mitigating risk while responding to an evolving threat landscape.

1 INVEST IN RISK-BASED VULNERABILITY MANAGEMENT

At a time when cyber threats are increasing in both frequency and sophistication, many agencies continue to rely on reactive security measures or "good enough" risk management, leaving them vulnerable to potential cyber attacks. Government agencies often find themselves drowning in a sea of security alerts, while lacking the capacity to effectively identify and prioritize the critical ones. Federal agencies can no longer rely on "good enough" security. Rather, agencies must take a proactive stance and implement a holistic security approach.

Risk-based vulnerability management (VM) is a process that reduces vulnerabilities across the attack surface by prioritizing remediation based on risk. It helps agencies protect expanding networks and prevent breaches, with continuous assessments that give federal governments an accurate view of all assets and vulnerabilities in their environment that could be exploited. It enables security teams to prioritize critical vulnerabilities for remediation and make better risk-reduction decisions. With the complexity of infrastructures and an increasing reliance on technology, risk-based VM is more critical than ever.

Manage vulnerabilities with Tenable

Tenable offers cloud-based or on-prem solutions for risk-based VM with the industry's most comprehensive coverage — with specific solutions including FedRAMP-authorized Tenable Vulnerability Management (formerly Tenable.io) and Tenable Web App Scanning (formerly Tenable.io Web Application Scanning), as well as Tenable Security Center (formerly Tenable.sc) for on-prem environments and Tenable OT Security (formerly Tenable.ot) for securing critical infrastructure.

Tenable Vulnerability Management solutions provide unified visibility and a continuous view of all assets, both known and previously unknown. Using a combination of active scanning, agents, passive monitoring, cloud connectors and configuration management database (CMDB) integrations, Tenable will discover a wide range of assets, ensuring agencies have the visibility they need. With coverage for more than 77,000 vulnerabilities, Tenable has the industry's most extensive common vulnerabilities and exposures (CVE) and security configuration support to help agencies understand all their exposures. To ensure high risk vulnerabilities are remediated first, Tenable VM solutions provide easy to understand risk scores so agencies can quickly assess risk and make informed remediation decisions.

Tenable Web App Scanning further expands vulnerability coverage by providing full visibility of IT, cloud and web application vulnerabilities in a single platform. It offers simple, scalable and automated vulnerability scanning for web applications, including comprehensive and accurate vulnerability scanning, from the Open Worldwide Application Security Project (OWASP) to top 10 risks and vulnerable web components.

Tenable OT Security provides agencies with unmatched visibility across IT and OT security operations, giving them complete visibility, security and control of their OT networks and helping agencies bridge the gap between IT and OT environments.

2 SAFEGUARD CRITICAL INFRASTRUCTURE

Safeguarding critical infrastructure is crucial to maintaining the stability and security of our society. Unfortunately, critical infrastructure is a desirable target for nation-state actors, hacktivists and other threat actors. With a single successful attack, these actors can cause immense damage, making it essential to prioritize the security of our critical infrastructure.

One significant issue in securing critical infrastructure is the convergence of information technology (IT) and operational technology (OT) environments. Many agencies lack visibility into their OT environments, and securing converged IT and OT is not always a priority. Requests for proposal (RFPs) and procurement vehicles rarely even include OT cybersecurity requirements, exacerbating the problem. According to a Gartner® report "attacks on organizations in critical infrastructure sectors have increased dramatically, from less than 10 in 2013 to almost 400 in 2020 — a 3,900% change".[3] Adding to the challenge is the fact that critical infrastructure is often under-protected due to a reliance on outdated technologies. Technologies beyond end-of-life that are no longer supported by vendors can create:

- **Security vulnerabilities resulting from a lack of frequent updates**
- **Incompatibility with new solutions, causing performance degradation**
- **Compliance issues**
- **Business continuity risks**

In June 2019, the GAO reported that several of the federal government's most critical legacy systems used outdated languages as well as unsupported hardware and software with known security vulnerabilities.[4]

To manage internal operations, agencies continue to layer more technology, including cloud computing, robotic process automation, data analytics, artificial intelligence and virtual and augmented reality. However, the fragmented understanding of risk due to siloing of information and differing levels of expertise and resources between agencies or departments can lead to inconsistent risk assessments, limited sharing of threat intelligence and misaligned allocation of resources.

Adding to the challenges, limited budgets make it difficult for agencies to invest in the technology, human capital and training necessary to maintain a proactive stance. This leads to unperformed risk assessments, vulnerability scanning and security awareness training. As of December 2022, only 40% of the GAO's 236 recommendations on improving cyber risk in federal agencies since 2010 have been implemented.[5]

Despite these challenges, executing a strategy to safeguard critical infrastructure can help mitigate risk and protect agencies and the constituents they serve. The right tools provide the visibility, threat tracking and situational awareness essential to securing critical infrastructure.

Reducing cyber threat exposure

Tenable OT Security supports the security of critical infrastructure. With Tenable OT Security, agencies can immediately discover all devices on their network, whether they are active or dormant, and get visibility into their make, model and firmware version. Tenable OT Security also tracks risk scores and identifies vulnerable assets, giving agencies a simple method to mitigate threats and make the best use of their security team's time. With deep situational awareness across all global sites and their respective assets — from Windows servers to programmable logic controllers (PLC) backplanes — in a single interface, Tenable OT Security provides the visibility necessary to protect our nation's critical infrastructure.

3 IMPLEMENT A ZERO TRUST STRATEGY

With the rise of cyber attacks, perimeter-based cybersecurity is no longer adequate. To meet evolving challenges, agencies should rely on a Zero Trust approach to cybersecurity, which has become essential to protecting against attacks that leverage misconfigurations. Zero Trust is built on a trust-no-one approach to disrupting attack paths and safeguarding agencies against attacks.

Factors driving the need for Zero Trust cybersecurity

Seen as a critical tool in updating security standards, Zero Trust is mandated by EO 14028. This mandate has been driven by the increased number and sophistication of threats against federal agencies and the need to protect critical infrastructures. In addition, the need for situational awareness built on a granular view of network activity is essential to enable faster incident response.

A unique factor driving the shift to Zero Trust cybersecurity is the rise of remote work. The COVID-19 pandemic created a "rush to remote" situation that led to technical debt. Employees may access federal networks via their personal devices, which lack firewalls and other security software. Employees may also use public networks, which are insecure and can be exploited by malicious actors while VPNs also remain vulnerable. Compounding this, employees typically don't receive adequate security awareness training, so they don't know how to secure their home Wi-Fi or ensure that multi-factor authentication is used while accessing networks.

Typical vulnerabilities that malicious actors may exploit include unsecured home connections, devices that may not be protected by the same security protocols as government-issued devices and remote access tools that are preferred targets of cybercriminals. In fact, 94% of Department of Defense (DoD) employees report that their personal devices are not approved by the agency.[6]

Implementing a Zero Trust strategy

To implement a Zero Trust strategy, it's important to verify every possible factor about a user or device before granting access to various networks and systems. Continuously assessing which resources are susceptible to a breach is essential.

The Tenable Identity Exposure (formerly Tenable.ad) and Tenable Vulnerability Management solutions help support this strategy. Tenable Vulnerability Management provides foundational visibility into the network, vulnerability prioritization to stop attacks before they happen and AD security to stop lateral movement. And with Tenable Identity Exposure, organizations can take a proactive approach to identity security and ensure that a Zero Trust strategy is in place. Both are built on a trust-no-one, verify-everything approach and enable the continuous verification required to maintain Zero Trust architectures and Cybersecurity and Infrastructure Security Agency (CISA) policies and mandates.

4 SECURE ACTIVE DIRECTORY (AD)

AD is a central component of an organization's IT infrastructure, providing a single point of access for network resources and system privileges. This makes it a prime target for attackers looking to gain access to sensitive data or compromise critical systems. To keep AD safe and secure, it's critical to have effective strategies and tools in place to prevent and detect attacks.

One of the main risks around AD is privilege escalation. Attackers will use whatever method they can to gain access to an administrator account, which will give them access to sensitive data and allow them to make changes to systems across the network. Credential theft is another common technique used by attackers who use pass-the-hash, Kerberos and brute force attacks to steal legitimate credentials. With a set of credentials, attackers can explore the network undetected and carry out their malicious activities.

Another threat to AD is malware propagation. Attackers can use access to an AD domain to spread malware across the entire network, with the potential to control the entire domain if they gain access to a domain controller. Poor visibility is also a risk, as AD delivers a centralized view of the entire network that attackers can use to hide their activities and remain undetected for long periods of time. On top of this, misconfigurations can leave the door open for attackers to walk in and query.

To keep AD safe and secure, it's vital to enforce local administrator password solutions (LAPS) and privileged access management (PAM), and promote best authentication practices such as multi-factor and strong password policies. In addition, using effective tools such as Tenable Identity Exposure can help to prevent and detect attacks.

How Tenable Identity Security Can Help

1

Find and fix existing weaknesses

- Immediately discover, map, and score existing weaknesses
- Follow our step-by-step remediation tactics and prevent attacks

2

Maintain hardened security settings

- Instantly detect new weaknesses and misconfigurations
- Break attach pathways and keep your threat exposure in check

3

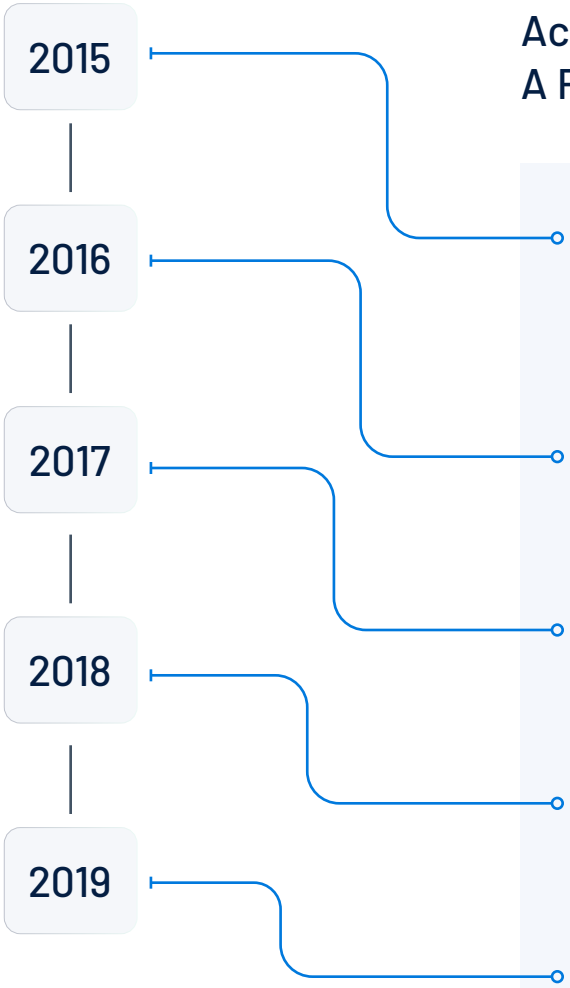
Detect & respond to attacks in real-time

- Get real-time alerts and actionable remediation plans on AD attacks
- Visualize notifications and trigger responses in your SIEM / SOAR / SOC
- Honeypot configurations to attract and distract threat actors

4

Enhance incident response & threat investigations

- Drill down into the most comprehensive security tracker for AD
- Search and correlate AD changes at object and attribute levels
- Easily visualize attack pathways for AD objects and assets



Active Directory: A Prime Threat Vector

US Office of Personnel Management (OPM): Attackers used stolen credentials to access the agency's AD and compromise the personal information of millions of federal employees and contractors.

Department of Justice (DOJ): Attackers used stolen credentials to access the agency's AD and move laterally through the network to access sensitive information.

US National Security Agency (NSA): Attackers used stolen credentials to access the agency's AD and move laterally through the network.

US Department of Homeland Security (DHS): Attackers used stolen credentials to access the agency's AD and exfiltrate sensitive data.

US Department of Defense (DoD): Attackers exploited a vulnerability in the DoD's AD and compromised the personal information of ~30,000 military and civilian personnel.

Tenable Identity Exposure is a powerful tool that can help agencies to keep their identity stores, such as Active Directory safe and secure. It provides comprehensive vulnerability scanning, discovery, and prioritization of weaknesses in existing AD domains. This helps to reduce exposure to attacks and provides step-by-step guidance to address issues. Tenable Identity Exposure also enables real-time detection and response to AD attacks, enriching security information and event management (SIEM), Security Operations Center (SOC) or Security Orchestration, Automation and Response (SOAR) with insights that enable fast remediation and mitigation.

5 LEVERAGE CLOUD SOLUTIONS THAT ACHIEVE FEDRAMP COMPLIANCE

More organizations are adopting cloud solutions to store their data and run their operations. The federal government is no exception, with many agencies leveraging cloud services to modernize their infrastructure and improve efficiency. However, with the shift to the cloud comes new cybersecurity risks. One way that agencies can ensure their cloud solutions are secure is by using solutions that meet the Federal Risk and Authorization Management Program (FedRAMP) compliance.

FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization and continuous monitoring for cloud products and services. By using FedRAMP-compliant solutions, agencies can be confident that their cloud solutions meet strict security requirements through rigorous testing and validation.

Leveraging FedRAMP-compliant solutions — such as Tenable Vulnerability Management and Tenable Web App Scanning — provides several benefits to federal agencies:

- **Improve cybersecurity posture** by ensuring that cloud solutions are secure and protected from cyber threats. With comprehensive and accurate vulnerability scanning, agencies can identify and remediate any vulnerabilities in their web applications.
- **Help reduce costs** by avoiding the need to develop bespoke security solutions. By leveraging pre-existing solutions, agencies can save time and money.
- **Increase scalability** as agencies grow and their needs change. FedRAMP-compliant solutions are designed to be scalable and flexible, allowing agencies to adapt to shifting requirements.
- **Promote agency collaboration** by using a standardized approach to security. This can help to improve efficiency and streamline operations.
- **Ensure compliance with federal regulations** by using solutions that have already been approved by the government.

FedRAMP authorized Tenable Vulnerability Management and Tenable Web App Scanning provide full visibility of IT, cloud and web app vulnerabilities in a single platform. With continuous, always-on asset discovery and assessment, built-in prioritization and intuitive dashboards visualizations and reports, agencies get immediate insight to reduce risk and stop attacks before they happen.

Overcoming federal compliance hurdles with ease

Federal networks use more technology, including cloud and hybrid-cloud environments, to manage internal operations and communicate with other government entities. However, relying on outdated technologies beyond end-of-life that are no longer supported by vendors can lead to compliance issues, security vulnerabilities and business continuity risks – all amid a rise of reported security incidents.

Agencies dealing with many regulations and sensitive data have to spend a great deal of time on compliance. These necessary efforts are costly and time-consuming, monopolizing resources that are not available for proactive security. "Audit fatigue" is a vulnerability in itself. As resources are devoted to audit preparation, security professionals are at risk of distraction from their mission to protect the agency.

Vulnerability prioritization is critical, and using risk-based VM scans helps prioritize the vulnerabilities that pose the biggest threat to federal entities.

As federal agencies face complex regulatory requirements and an expanding attack surface, investing in risk-based VM will help agencies protect citizens, data, and systems from cyber attacks.

The number of attacks targeting the government sector increased by 95% worldwide in the second half of 2022 compared to the same period in 2021.[7]

And as benchmarks are released from source authorities, Tenable Research implements the guidance in its audit language. These audit files are executed and evaluated by Tenable sensors, and reported in Tenable products. Tenable Research has published 1155 audits covering 443 benchmarks from source authorities and vendors that include Center for Internet Security, the United States Defense Information Systems Agency, and Microsoft.

LEVERAGING A TRUSTED PARTNER TO MANAGE ATTACK SURFACES

Federal agencies hold massive amounts of sensitive data, making them attractive targets for malicious actors. To keep attackers at bay, agencies need to proactively and continuously manage their attack surfaces. Tenable, a trusted member of the CISA Joint Cyber Defense Collaborative (JCDC), offers the continuous visibility, vulnerability prioritization and identity security required to maintain Zero Trust architectures and comply with CISA policies and mandates.[8]

Tenable advises the National Institute of Standards and Technology (NIST) on exposure management needs to improve the cybersecurity of federal agencies.[9] We help agencies control their attack surfaces by providing a comprehensive dashboard that simplifies exposure management. This dashboard delivers vulnerability scoring that makes it easy to see where the agency is most exposed. This way, agencies can accurately prioritize their responses and keep their systems secure.

Risk-based vulnerability management for federal agencies

Tenable helps federal agencies gain full visibility into their attack surface so they can identify, investigate and prioritize vulnerabilities proactively and continuously. With FedRAMP-authorized solutions for VM and web application scanning, as well as solutions for on-prem VM, OT security and AD security, federal agencies can ensure they have the context and visibility they need to reduce risk and stop breaches.

Seamless integration with existing cybersecurity investments

Tenable's solutions are designed to seamlessly integrate with existing cybersecurity investments. This allows agencies to unify data across silos and build a comprehensive understanding of the risk exposure that accounts for all users and attack surfaces across continuously changing hybrid environments. Our solutions extend an agency's existing tools and VM to create a proactive management of risk exposure.

SCHEDULE A DEMO WITH TENABLE TODAY

The level of risk faced by federal agencies continues to grow as organizations allow more devices, networks, systems and partners to access their infrastructures. As a result, agencies need a partner they can trust to help them understand and manage their attack surfaces continuously.

Request a demo of Tenable today and discover what proactive security looks like for your agency.

Schedule a call with a sales rep today to learn more about how Tenable can help your agency stay ahead of attackers.

[1] *"Significant Cyber Incidents," Center for Strategic & International Studies, Feb. 2023*
[2] *Executive Order on Improving the Nation's Cybersecurity, May 2021, whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/*
[3] *Predicts 2022: Cyber-Physical Systems Security — Critical Infrastructure in Focus," Gartner Research, 17 November 2021, By Katell Thielemann, Wam Voster, Barika Pace, Ruggero Contu, Richard Hunter, gartner.com/en/documents/4008351. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved*
[4] *Agencies Need to Develop and Implement Modernization Plans for Critical Legacy Systems," GAO, April 2021, gao.gov/assets/gao-21-524t.pdf*
[5] *Cybersecurity High-Risk Series: Challenges in Protecting Privacy and Sensitive Data," GAO, Feb. 2023, gao.gov/products/gao-23-106443*
[6] *"Most feds bring own devices to work without agency approval: Report," CISO Mag, July 2018, cisomag.com/most-feds-bring-own-devices-to-work-without-agency-approval*
[7] *"7Unprecedented Increase in Cyber Attacks Targeting Government Entities in 2022, CloudSek, Dec. 2022 https://www.cloudsek.com/whitepapers-reports/unprecedented-increase-in-cyber-attacks-targeting-government-entities-in-2022*
[8] *"Changing the Cybersecurity Paradigm: A Unified Cyber Defense," Joint Cyber Defense Collaborative, March 2022, cisa.gov/sites/default/files/publications/JCDC_Fact_Sheet.pdf*
[9] *National Institute of Standards and Technology, U.S. Department of Commerce, 2023, nist.gov*