FORTRA

A Proactive Approach To Federal Cybersecurity

A Proactive Approach to Federal Cybersecurity

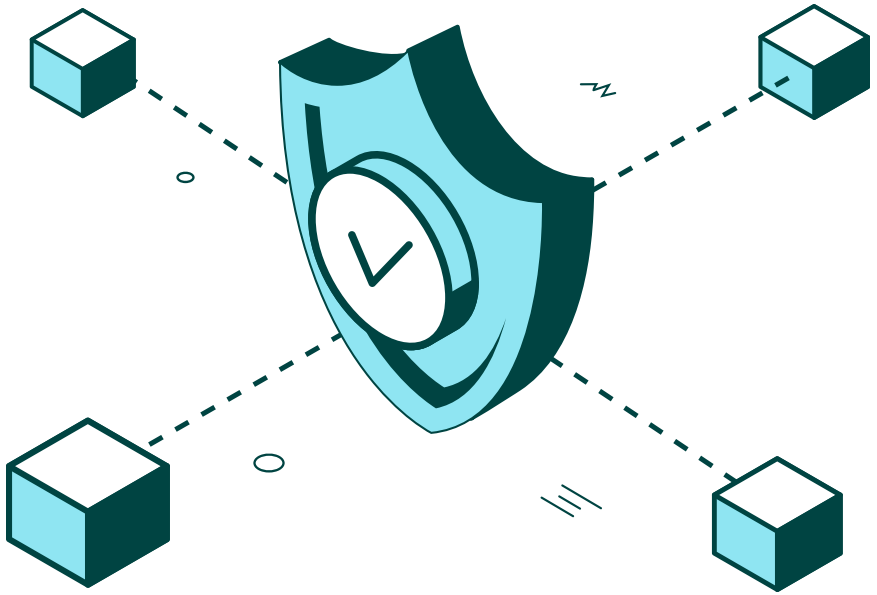
After countless headlines, government alerts, and warnings from experts, the message could not be any clearer: Cybersecurity events continue to grow in number and sophistication. As the number of threats grows, so does the boldness of cyber criminals.

The White House released an Executive Order on Improving the Nation's Cybersecurity that underscores the federal government's laser-like focus on tackling cybersecurity issues. The Executive Order aims to help federal government agencies:

- Remove barriers to sharing threat information
- Modernize federal cybersecurity
- Enhance software supply chain security
- Establish a cyber safety review board
- Standardize the government playbook for responding to vulnerabilities and incidents
- Improve detection of vulnerabilities and incidents on federal networks
- Improve the government's investigative and remediation capabilities

The order urges agencies to move toward a Zero Trust Security Model, which requires continuous verification of the operational picture through real-time information from multiple sources to control technology access and other system responses. Zero Trust is gaining usage in private industry to help thwart increasingly sophisticated attacks by eliminating implicit trust in any one element, node, or service.

Federal agencies must step up their security games, complying with both existing and emerging regulations related to information security. This guide offers a maturity matrix to help agencies determine the health of their IT security infrastructure and outlines infrastructure protection focus areas that can help proactively achieve and exceed compliance.



What is Your Level of Security Maturity?

Attaining compliance with federal security guidelines can often feel like boiling the ocean — a Herculean task. Any effort must start with an honest assessment of an organization, its IT team, and security protocols to discover the logical next steps to reach a higher maturity level.

It's important to evaluate the security maturity level of your federal agency to ensure you get maximum value from your efforts. The matrix below will help you determine what phase your organization falls into and recommended areas to focus your efforts.

	EARLY	MATURING	MATURE
Team Attributes	• Small team, part of larger IT organization • Reactive focus on security • Not enough staff to accomplish everything	• Small- to mid-sized team • Starting to take proactive steps to reduce risk	• Large team • Fostered culture of security learning • Experts on staff
Agency Attributes	• Limited security awareness from leaders • No sustained agency-wide security focus	• Security team developing influence within agency • Meeting compliance requirements • Security-focused leadership is emerging	• Risk awareness is pervasive • Security is a part of day-to-day life
Team Member Specialization	• Generalists managing IT and security • Little, if any, expert knowledge	• Starting to specialize on areas of security (i.e., network-only security admin)	• Specialists, highly skilled individuals in key roles (SIEM admin, pen testers, Red Teamers, etc.)

What is Your Level of Security Maturity?

	EARLY	MATURING	MATURE
Types of Solutions in Place	• Firewall / Antivirus • Spam filter / Web proxy • Vulnerability management	• Log management • Security awareness training	• Covering most if not all the Top-10 critical controls • External threat intelligence
Retained Services	• Managed application security	• MSSP • Training • Penetration testing	• Cyber Maturity Assessment • Red Teaming
Recommended Areas of Focus	• Vulnerability Scanning • Security Information and Event Management (SIEM) • Server-Level Protection / Antivirus • Security Policy Management	Same as early + • Penetration Testing Software • Penetration Testing Services • Web Application Scanning	Same as maturing + • Adversary Simulation • Red Teaming

No matter where your federal agency falls on the table above, there will always be a need to proactively fine tune your security program to stay ahead of attackers. The following includes important considerations for each maturity level to help you pinpoint the next best step for your team.

EARLY: Vulnerability Management Best Practices

Security vulnerabilities are an endemic part of technology that the entire sector must constantly battle. According to the National Vulnerability Database (NVD), over 19,000 vulnerabilities were discovered in 2020, and over 20,000 were found in 2021. The goal of cybersecurity is no longer eradicating vulnerabilities but managing vulnerabilities effectively to minimize potential attack surfaces. Vulnerability management, which focuses on uncovering these security weaknesses, is critical for the creation of a sturdy foundation for any cybersecurity program.

Vulnerability Management Tools

Effective vulnerability management tools are critical to track the current security status of an entity. The most common type of solution is a vulnerability scanner, an automated tool that scans network or web applications to identify vulnerabilities. An effective solution uses external intelligence to help evaluate these vulnerabilities and generates a report that prioritizes them based upon risk and a standardized or proprietary scoring system.

Vulnerability scanning is required for many different federal and compliance regulations, including PCI DSS, HIPAA, SOX, and FISMA. Vulnerability management solutions, like Frontline VM, are particularly useful because they can be fully automated and are easy to use. Organizations can run scans frequently to get an up-to-date picture of the security of their environment, which can change daily, particularly when software or hardware is being added or updated.

Scanners aren't the only vulnerability management tools. Other, more specialized tools can also help to identify security weaknesses. For example, application developers commonly use Dynamic Application Security Testing (DAST) tools, like beSTORM, to perform black box fuzzing, which can uncover bugs through random data injection. They may also use Static Application Security Test (SAST) tools, like beSOURCE, to examine their application's implementation (the source code). This analysis includes a full source code audit (also referred to as a code review).

Agencies also need the right antivirus tools for their IT environments. Many agencies run some combination of Windows, Linux, AIX, or IBM i. But most antivirus software solutions are designed just for Windows, which can leave other environments susceptible to worms and malware threats. Powertech Antivirus provides the only commercially available server-level antivirus solution, with native scanning for IBM Power OS Systems, including IBM i, AIX, Linux on Power, and LinuxOne.

MATURING: Penetration Testing Best Practices

Penetration tests use the same techniques as an attacker to uncover and safely exploit vulnerabilities to determine whether a threat actor could use a security weakness to successfully breach an environment or gain access to other parts of the system through privilege escalation or other means. Pen tests measure the feasibility of systems or end-user compromise and evaluate any related consequences such incidents may have on the involved resources or operations.

Once a penetration test has been completed, a report is created that details the level of risk vulnerabilities pose based on how effectively testers were able to exploit them. These reports help to demonstrate the efficacy of defensive mechanisms and end-user adherence to security policies. Additionally, this gives federal agencies a path forward for remediation.

Though they are often mistaken as synonymous processes, penetration tests and vulnerability scans have several marked differences. Penetration testing builds on the work of vulnerability management, taking the next steps to evaluate the security of an IT environment and further prioritize risk.

Penetration Testing Teams

Penetration testing teams can be either inhouse or external, third-party services. Larger entities often invest in a full in-house team to bolster their vulnerability management program with more consistent initiatives, particularly for maintaining federal compliance. In-house teams can also help to quickly follow through on any remediation measures.

However, expert penetration testers can be a scarce resource in government entities, so creating a full in-house team may be challenging. According to the 2021 Cybersecurity Workforce Survey, 60% of study participants reported that the cybersecurity workforce gap is placing their organizations at risk. As a result, it's also common to have smaller security teams that handle basic, routine tests, while third-party services are used for more complex tests.

Even those with full in-house teams may employ third-party services for various reasons. For example, it may be difficult for internal IT or security teams to see every problem because, as in everyday life, being habituated to the situation or environment can make it difficult to see the forest for the trees. Pen testing services offer an external point of view, providing a fresh perspective and objectively identifying security issues that may have been overlooked. Additionally, since third-party services are executing penetration tests and other security assessments full time, they can stay up to date on the latest attacks, in addition to providing unique combinations of tactics and techniques.

Penetration Testing Tools

Just as threat actors employ tools to compromise an environment, pen testers utilize tools like Core Impact to streamline the process of exploiting vulnerabilities. For example, there are tools that help create sophisticated spear phish for campaigns to gauge employees' ability to identify such attacks. Other specialized pen testing tools include port scanners, password crackers, SQL injection tools, and Wi-Fi auditors. Other tools may offer multiple features to centralize the testing process.

Some tools can even automate routine tasks so pen testers can concentrate on more dynamic issues. Such penetration testing tools can be used by security team members who may not have an extensive pen testing background, using them for tests that are easy to run, but essential to perform regularly, like validating vulnerability scans.

MATURE:
Red Teaming Best Practices

Red Teaming is an offensive exercise that tests an organization's defenses by fully simulating a cyber-attack scenario. The concept of Red Teaming traces its roots to military planning, as leaders realized there were circumstances not considered in the original planning that could jeopardize their success. Confronting the intended approach with unpredictable events is now a recognized method of critical testing. Red Teams translate perfectly to the cybersecurity realm and are used to challenge the strength of cybersecurity programs, particularly their defensive assumptions.

The Distinction Between Penetration Testing and Red Teaming

While penetration testing does mimic an attacker in the sense that they are trying to gain a foothold or escalate their privileges within an IT environment, the focus is primarily on whether such actions are possible. Since an actual attacker would not limit movements to one specific aspect of an infrastructure, a penetration test is limited in how well it represents a threat actor in the wild.

Red Teaming emulates a real-world scenario with a broader scope but clear objectives. These teams take on the offensive role of an attacker who will have to evade detection and beat security controls, including the federal agency's own security team. While the goal of a penetration test is exploitation, the goal of a Red Team exercise is testing the ability to successfully detect and respond to attacks.

The impact and effectiveness of Red Teams can be amplified with threat emulation software and attack kits that provide structure to execute a threat plan and the tactics and techniques of an adversary in a network. Tools like Cobalt Strike provide a flexible post-exploitation framework that can emulate embedded adversaries.

Adopt a Layered Approach to Cybersecurity

While individual infrastructure protection solutions are valuable, they are even more effective when used in tandem. Together, they cover every layer of complexity to create a mature security program and ensure a federal organization can overcome cybersecurity challenges.

For a security operations team to be successful, they must not only reduce the attack surface through preventative controls but be able to detect and respond to threat activity before serious impact is felt. A proactive approach serves as the first line of defense, providing significant obstacles that make breaking in so labor intensive that the vast majority of attackers, who always look for the easiest wins, won't even attempt it.

Ultimately, a well-rounded program of prevention, detection, and response separates federal agencies that are pushed around by threats from those that push back against threats.

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

fta-cs-gd-1022-r1-79d