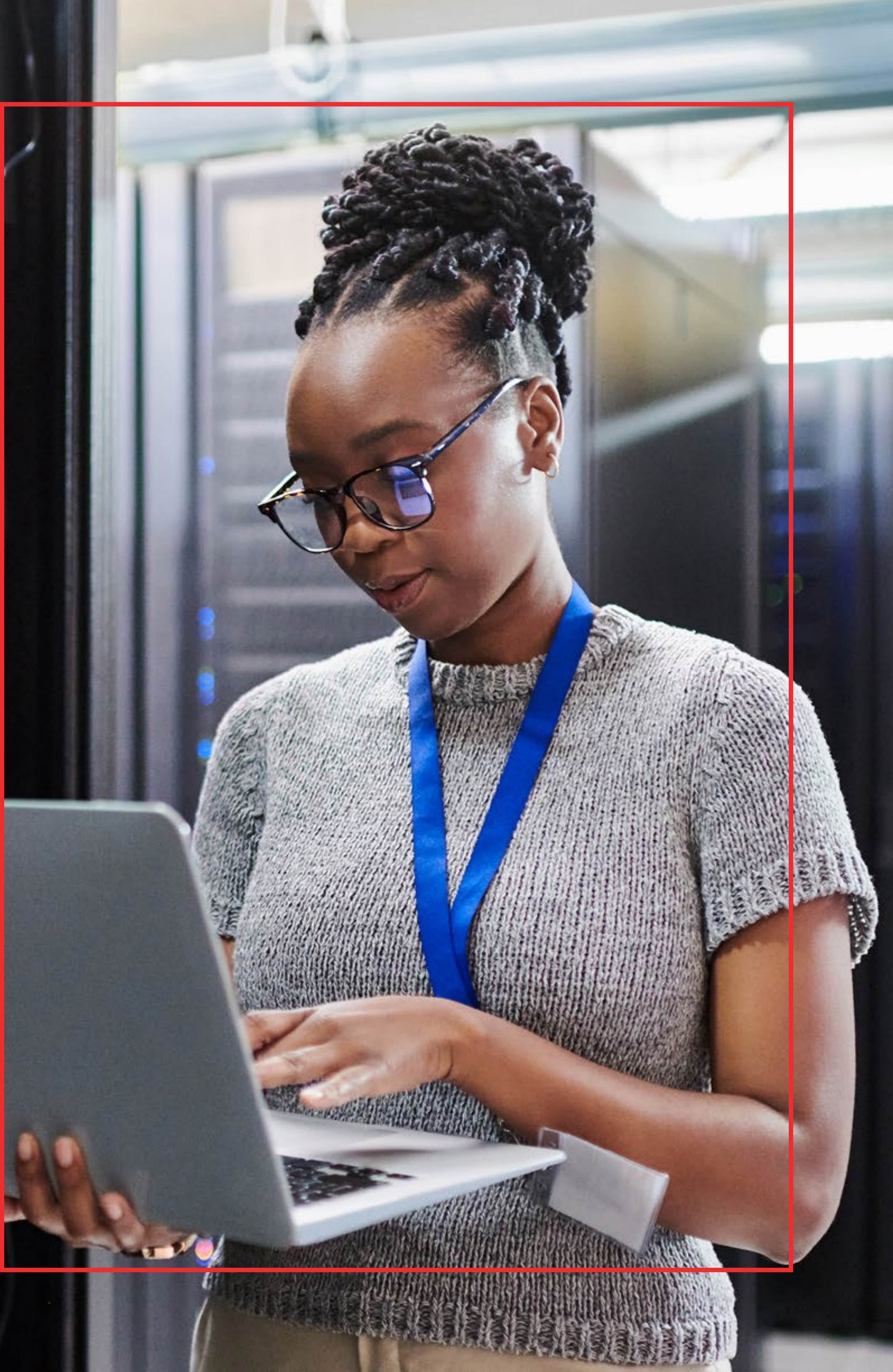
Breaking down the CISA Directive: How federal agencies can prioritize actions to remediate known vulnerabilities quickly and at scale

Practical advice on how federal agencies can gain visibility into their environment and remediate known vulnerabilities while meeting the directive's deadlines.



CHAPTER 1:

Security at the speed of cyber: What is CISA's Binding Operational Directive (BOD) 22-01?

The Biden Administration is continuing efforts to adopt new cybersecurity protocols in the face of ongoing attacks that threaten to disrupt critical public services, infringe on citizen data privacy and compromise national security.

On November 3, 2021, the Cybersecurity and Infrastructure Security Agency (CISA) issued a **directive** for federal agencies and contractors who manage hardware or software on an agency's behalf to fix nearly 300 known cyber vulnerabilities that malicious actors can use to infiltrate and damage federal information systems. These known exploited vulnerabilities fall into two categories, each with a deadline for remediation:

- 90 vulnerabilities that were discovered in 2021 must be remediated by November 17
- About 200 security vulnerabilities that were first identified between 2017 and 2020 must be remediated by May 3, 2022

As part of the directive, CISA also created a **catalog of known exploited vulnerabilities** that carry "significant risk" and outlined requirements for agencies to fix them. The catalog includes software and configurations supplied by software providers like SolarWinds and Kaseya, and large tech companies like Apple, Cisco, Google, Microsoft, Oracle and SAP.

Improving the nation's cybersecurity defenses continues to be a top priority as the country has experienced an unprecedented year of cyberattacks. Malicious actors are continuing to target remote systems and prey on known vulnerabilities as the pandemic continues, leading to public service disruptions in telecommunications and utilities.

This directive comes just shy of six months since President Biden issued his **Executive Order on Improving the Nation's Cybersecurity**, which aims to modernize cybersecurity defenses by protecting federal networks, strengthen information-sharing on cyber issues, and strengthen the United States' ability to quickly respond to incidents when they occur.

While the Biden Administration and many federal agency heads agree that these actions are necessary to improve cybersecurity protocols — they can be extraordinarily difficult to implement without the right tools.

In the next section, we will explore how federal agencies and their security teams can gain visibility across distributed environments to remediate vulnerabilities outlined in the directive.

CHAPTER 2:

Gaining visibility into federated IT environments

While most federal agencies are headquartered in Washington, D.C., field offices and agency staff are spread across the country, using many different endpoints (laptops, desktops and servers) to access federal networks. This distributed IT environment can make it difficult for CISOs and their security teams to gain visibility into their agency's environment in real time.

To comply with CISA's BOD 22-01, security teams first need to gain visibility across federated IT environments and be able to answer a few basic questions, including:

- How many endpoints are on the network?
- Are these endpoints managed or unmanaged?
- Do any known exploited vulnerabilities cataloged in the directive exist in our environment? If so, do we currently have the tools to patch them quickly and at scale?
- Do we have the capability to confirm whether deployed patches were applied correctly?

While these questions may seem straightforward, they often take agencies weeks or months to answer due to a highly federated IT environment and the nature of IT management, which often includes tool sprawl and conflicting data sets — which is at odds with the aggressive timelines outlined in the directive.

With Tanium, CISOs and their security teams can discover previously unseen or unmanaged endpoints connected to federal networks, and then search for all applicable Common Vulnerabilities and Exposures (CVEs) listed in the directive in minutes. With Tanium, it only takes a single agent on the endpoint to obtain compliance information, push patches and update software. Tanium provides a "single pane of glass" view to help align teams and prevent them from spending time gathering outdated endpoint data from various sources.

As CISA has committed to maintaining the catalog and alerting agencies of updates for awareness and action, having a unified endpoint management platform that provides visibility across an organization gives CISOs and their teams the tools they need to scan and patch future vulnerabilities at scale.

In the next section, we will explore how federal agencies and their security teams can prioritize actions and deploy patches to meet deadlines outlined in the directive.

CHAPTER 3:

Prioritizing actions and patching known vulnerabilities quickly

Once agency heads and their security teams have a clear picture of the state of their endpoints, the next step is to pinpoint known vulnerabilities and fix them fast based on associated deadlines in the directive.

With Tanium, federal agencies can search for the specific vulnerabilities listed in the directive and then patch those vulnerabilities in minutes, while having the confidence that patches were applied correctly. As a single lightweight agent, Tanium doesn't weigh down the network. Remediation typically takes less than a day if an agency is already using Tanium. Existing customers should reference **this step-by-step technical guidance** on how to address the vulnerabilities laid out in the directive.

In addition to fixing known vulnerabilities, the directive also outlines other actions federal agencies must take, including:

Reviewing and updating internal vulnerability management procedures within 60 days. At a minimum, agency policies must:

- Pave the way for automation around a single source of truth with high-fidelity data and remediate vulnerabilities that CISA identifies within a set timeline
- Assign roles and responsibilities for executing agency actions to align teams around a single source of truth
- Define necessary actions required to enable prompt responses
- Establish internal validation and enforcement procedures to ensure adherence to the directive
- Set internal tracking and reporting requirements to evaluate adherence to the directive and provide reporting to CISA, as needed

Reporting on the status of vulnerabilities listed in the catalog.

- Agencies are expected to automate data exchanges and report their respective directive implementation status through the CDM Federal Dashboard

As new threats and vulnerabilities are discovered, CISA will update the catalog of known vulnerabilities and alert agencies of updates for awareness and action.

Many federal agencies already use Tanium to provide visibility and maintain compliance across their distributed IT environment. Federal agencies can count on Tanium to be a valuable tool in discovering, patching and remediating future known critical vulnerabilities.

CHAPTER 4:

Tanium in action: scanning distributed networks and remediating at scale

While CISA has previously imposed cybersecurity mandates on federal agencies to immediately fix a critical software problem, this new directive is notable for its sheer scope and respective deadlines. Leveraging Tanium, federal agencies and contractors who manage hardware or software on an agency's behalf can patch known critical vulnerabilities and comply with the deadlines in a fraction of the time.

The Tanium platform unifies security and IT operations teams using a "single pane of glass" approach of critical endpoint data, so that federal agencies can make informed decisions and act with lightning speed to minimize disruptions to mission-critical operations.

With Tanium, you can get rapid answers, real-time visibility and quickly take action when addressing current vulnerabilities in BOD 22-01. As CISA adds more vulnerabilities to the catalog, you can have confidence that Tanium is constantly checking for compliance and patching your endpoints quickly across your environment.

To learn more about how Tanium can help your agency remediate known vulnerabilities outlined in the CISA directive, visit Tanium.com/cisa.