Your Agency's Zero Trust Roadmap

The language of cybersecurity can be complicated and full of terminology that a layperson may struggle to understand. But protecting computer systems from cyberthreats – especially government systems – is increasingly critical.

To emphasize the point, in May 2021 the President released an "Executive Order on Improving the Nation's Cybersecurity" that instructed federal agencies to implement numerous cyber protections, including transitioning to a "zero trust" security architecture. The Office of Management & Budget (OMB) issued follow-up guidance in January 2022 that gave more detail.

So, what exactly does zero trust mean, and how can federal agencies implement it? The information below offers a shared language on what zero trust entails and practical steps you can take to adopt it.

Some of these steps may be beyond your specific purview, but we're hoping to give you a full picture of what zero trust requires.

5 Pillars: The Framework of Zero Trust

A core principle of zero trust is that no actor, device, system, network, or service operating outside or inside a security perimeter is automatically trusted. That means a federal agency should **verify anything and everything** that tries to access its network.

The OMB guidance divides zero trust into **five pillars** – Identity, Devices, Networks, Applications and Workloads, and Data – and agencies must implement certain protocols in each area. Below are checklists to guide your agency efforts. The OMB guidance offers more technical details.

Identity

- ☐ Employ identity management systems that apply to all users and integrate those systems with the agency's most used applications and platforms.
- ☐ Include strong multi-factor authentication (MFA) requirements as a key element in those identity management systems.
- ☐ Ensure that cyber tools can determine both whether someone has permission to access an agency system and what that person is authorized to see.

Multi-Factor Authentication: *a way to secure data & applications that requires a user to input two or more ID credentials (e.g., a password and your Personal Identity Verification [PIV]) before granting access*

Devices

- ☐ Follow updated federal guidance that explains how your agency should inventory its cloud-based assets — specifically, updated guidance being developed by the Cybersecurity & Infrastructure Security Agency (CISA) as part of its Continuous Diagnostics and Mitigation Program.
- ☐ Meet federal requirements for detecting cyber vulnerabilities on your agency's laptops, smartphones, and other devices and for reporting security gaps to CISA.

CISA: *federal agency established in 2012 that leads the national effort to understand, manage and reduce risk to our cyber and physical infrastructure*

Network/Environment

- ☐ Encrypt traffic across your agency's internal network and whenever users access the internet.
- ☐ Change HTTP website addresses to the more secure HTTPS version, for both public and private agency websites.
- ☐ Replace older encryption approaches with new CISA recommendations.
- ☐ Develop a zero trust plan that reflects the agency's unique operating circumstances, and submit it to OMB.

Encryption: *a way to secure digital data using one or more mathematical techniques, along with a password (or "key") that decrypts the information*

Applications Workloads

- ☐ Test the security of agency software internally in a comprehensive, rigorous way, using both automated analysis tools and expert analysis.
- ☐ Use third-party firms to independently test IT security as well.
- ☐ Create a welcoming, effective program that lets members of the public report vulnerabilities they notice in the agency's cybersecurity.
- ☐ Determine which applications should be accessible on the public internet — instead of using vehicles such as virtual private networks (VPNs) — and put them online in a safe manner.
- ☐ Have a complete understanding of all agency assets available on the public internet.
- ☐ Replace systems that require manual updates/patches with cloud-based systems that restrict manual changes.

IT Asset: *any hardware or software an agency uses, including operating systems, computers, and servers*

Data

- ☐ Chief data officers and chief security officers across the federal government create a joint committee to develop security guidelines for data management.
- ☐ Begin automating security management and enforcement.
- ☐ Audit access to any encrypted data stored in the cloud.
- ☐ Work with CISA to implement extensive abilities to share information and log network activity.

Data Management: *the process of collecting, keeping, and using data in a cost-effective, secure, and efficient manner*

Want to Know More?

The federal government has resources to guide your agency's transition to zero trust, including:

- "Executive Order on Improving the Nation's Cybersecurity" *Office of the President*
- "Strategy for Zero Trust Architecture" *Office of Management & Budget (OMB)*
- "Zero Trust Maturity Model" *Cybersecurity & Infrastructure Security Agency (CISA)*
- "Implementing a Zero Trust Architecture" *National Cybersecurity Center of Excellence (NCCoE)*

Learn more about how Presidio Federal and Cisco can help your agency achieve zero trust security at presidiofederal.com and at cisco.com.

A zero trust Center of Excellence (COE) at security.coe.presidiofederal.com offers additional expert guidance, and a virtual workshop provides hands-on instruction.

Further details are available at https://presidiofederal.com/events_c/zero-trust-strategy-planning-workshop/.

govloop CISCO PRESIDIO FEDERAL