Zero Trust Policy Memorandum

Zero Trust Policy Memorandum

Table of Contents

Introduction

In an era where cyber threats are growing in sophistication and scale, the security of government systems and sensitive data has never been more critical. To combat these evolving risks, the U.S. government has taken decisive action by adopting a Zero-Trust Cybersecurity Policy. On January 26, 2022, Shalanda D. Young, Acting Director of the Office of Management and Budget (OMB), issued a memorandum outlining the federal government's transition to a Zero-Trust Architecture (ZTA). This strategy mandates that federal agencies implement rigorous cybersecurity measures by the end of Fiscal Year 2024, ensuring that no user, system, or network is implicitly trusted—regardless of whether they operate inside or outside traditional security perimeters.

Zero Trust represents a fundamental shift in cybersecurity, emphasizing continuous verification, stringent access controls, and proactive threat mitigation. With cyber adversaries increasingly targeting critical government infrastructure, scientific research, and public services, a robust Zero-Trust framework is essential for safeguarding national security and maintaining public trust. This memorandum explores the key principles, components, and implementation strategies of the Zero-Trust Cybersecurity Policy, examining how it redefines the federal government's approach to digital security in an age of persistent cyber threats.

What is a Zero-Trust Cybersecurity Policy?

On January 26, 2022, Shalanda D. Young, appointed by President Joe Biden as Acting Director of the Office of Management and Budget, issued a memorandum on implementing a Zero-Trust Cybersecurity Policy. In this memorandum, Young directed the United States Government to adopt a Zero-Trust Architecture (ZTA) Strategy, requiring agencies to meet specific cybersecurity standards and objectives by the end of Fiscal Year (FY) 2024 to reinforce the government's defenses against increasingly sophisticated and persistent threat campaigns. These campaigns constantly jeopardize national security, public safety, and the economy while undermining public trust in government institutions.

The federal government undertakes unique and complex tasks daily, including maintaining critical infrastructure, conducting scientific research, engaging in diplomacy, and providing essential public services. To effectively accomplish these missions, the government must make intelligent and vigorous use of modern technology and security practices while preventing malicious cyber threats from disrupting them.

Zero Trust is a cybersecurity paradigm in which no actor, system, network, or service is inherently trusted, regardless of whether it operates inside or outside the security perimeter. The federal government must continuously evaluate and verify everything attempting to gain access to its systems. This strategy emphasizes stronger enterprise identity and access controls, including multi-factor authentication (MFA). Without secure, enterprise-managed identity systems, adversaries can hijack user accounts, infiltrate agencies, and steal data or launch attacks. ZTA also establishes reference points for access controls across the government, shielding agencies from sophisticated phishing attacks and guiding agencies to consolidate identity systems for consistent security enforcement and monitoring.

Zero-Trust Tenants

A significant tenet of Zero Trust Architecture is that no network is implicitly trusted, a principle that may contradict some agencies' current approaches to securing networks and associated systems. All traffic must be encrypted and authenticated as soon as possible.

Although Zero Trust concepts are not new, the transition from networks previously considered trusted is novel for many enterprises, including federal agencies. This transformation will be a long-term endeavor for the federal government, requiring continuous adaptation to new practices and technologies.

This memorandum mandates agencies to achieve specific Zero Trust security objectives by the end of Fiscal Year (FY) 2024. These objectives align with the Zero-Trust Maturity Model developed by the Cybersecurity and Infrastructure Security Agency (CISA). The strategic goals outlined in this memorandum revolve around CISA's five pillars:

1. Identity
2. Devices
3. Networks
4. Applications and Workloads
5. Data

The Elements of Zero-Trust

Identity: Agency personnel use enterprise-managed identities to access mission-critical applications. Phishing-resistant MFA safeguards personnel from sophisticated cyber threats. Agencies must employ integrated identity management systems that can be incorporated into applications and common platforms. Agencies should enforce robust MFA policies across their enterprises. When granting access to resources, agencies must consider at least one device-level signal in addition to identity-based authentication.

Devices: Agencies must maintain a comprehensive inventory of all authorized and operational devices used for official business and establish mechanisms to prevent, detect, and respond to security incidents on those devices. CISA's Continuous Diagnostics and Mitigation (CDM) program assists agencies in achieving asset visibility and cybersecurity awareness. Agencies must generate ongoing, reliable, and complete asset inventories, leveraging CDM tools. Additionally, agencies must ensure their Endpoint Detection and Response (EDR) tools comply with CISA's technical standards and provide necessary telemetry to CISA.

Networks: Agencies must encrypt all Domain Name System (DNS) requests and Hypertext Transfer Protocol (HTTP) traffic within their environments and work towards segmenting networks into smaller security zones. Agencies must resolve DNS queries using encrypted DNS whenever feasible. CISA's Protective DNS program supports encrypted DNS requirements. Agencies must also enforce HTTPS for all web and application programming interface (API) traffic. Furthermore, agencies must develop a Zero-Trust Architecture plan, in consultation with CISA, detailing their approach to network segmentation and submit it to OMB as part of their Zero-Trust implementation plan.

Applications and Workloads: Agencies must treat all applications as internet-connected, subjecting them to rigorous security testing and vulnerability assessments. Agencies must establish dedicated application security testing programs, engage third-party security firms for independent evaluations, and maintain a transparent public vulnerability disclosure program for internet-accessible systems. Additionally, agencies must designate at least one internal-facing Federal Information Security Modernization Act (FISMA) Moderate application to be securely accessible over the public internet.

Data: Agencies must implement comprehensive data classification and protection mechanisms. Federal Chief Data Officers and Chief Information Security Officers will collaborate to develop a Zero-Trust Data Security Guide. Agencies must automate data categorization and security responses, emphasizing tagging and access management for sensitive documents. Furthermore, agencies must audit access to encrypted data stored in commercial cloud environments and work with CISA to establish comprehensive logging and information-sharing capabilities, as outlined in OMB Memorandum M-21-31.

Deadlines

Agencies must meet the following deadlines outlined in the memorandum:

- Within 30 days of the memorandum's publication, agencies must designate a Zero-Trust strategy implementation lead.
- Within 60 days, agencies must refine their implementation plans, incorporating additional requirements identified in the memorandum. These plans, including budget estimates for FY24, must be submitted to OMB and CISA.
- Within one year, agencies must select at least one FISMA Moderate system that is not currently internet-accessible and enable its secure, full-featured operation over the internet.

Conclusion

As cyber threats continue to evolve in complexity and scale, implementing a Zero-Trust Cybersecurity Policy is imperative for the federal government. By adopting a Zero-Trust Architecture, agencies strengthen their digital defenses and reinforce public confidence in the security of critical systems. This transformation requires a fundamental shift in cybersecurity strategies, prioritizing continuous verification, robust identity management, encrypted communications, and proactive threat detection.

While the journey toward full Zero-Trust implementation presents challenges, it is crucial for securing government operations, protecting sensitive data, and ensuring national security. The OMB memorandum provides a structured framework with clear deadlines and objectives. The success of Zero-Trust adoption will depend on inter-agency collaboration, technological advancements, and a persistent commitment to cybersecurity resilience. In an era of inevitable cyber threats, Zero Trust is the federal government's most effective strategy for ensuring a secure and trustworthy digital future.

Endnotes

1. **Office of Mgmt. & Budget, Executive Office of the President,** Memorandum M-22-09 (Jan. 26, 2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
2. **Department of Defense,** *Zero Trust Reference Architecture* (Mar. 2021), https://dodcio.defense.gov/Portals/0/Documents/Library/(U)ZT_RA_v1.1(U)_Mar21.pdf.

Zero Trust Policy Memorandum

For more information, contact:

Authors

Lee Zeichner
CEO
lee@zra.com
(703) 868-8769

Zeichner Risk Analytics

4601 Fairfax Dr #1130, Arlington, VA 22203
(703) 351-1101

5661 Beaumont Avenue, San Diego, CA 92037
(703) 868-8769