White House to Introduce 'Zero Trust' Cybersecurity Policy to Federal Agencies

Oct 4, 2021

Reading Time : **3 min**

By: Erica Holland-Nesfield

What is Zero Trust Architecture?

Zero Trust architecture is a security framework that requires all users to be authenticated, authorized and continuously validated to gain access to an organization's network architecture. When deployed correctly, a Zero Trust architecture helps prevent successful data breaches by eliminating the concept of trust from an organization's network architecture. Zero Trust architecture is based on the principle of "never trust, always verify," as opposed to the traditional concept of "trust but verify."

The National Institute of Standards and Technology (NIST) released a second draft of its Zero Trust architecture publication in February 2020 and enhanced technologies to support the Zero Trust architecture are expanding.

What Would the OMB Draft Require for Government Agencies?

The OMB's draft Federal Zero Trust Strategy (the "OMB Draft") requires government agencies to achieve specific Zero Trust security goals by the end of Fiscal Year 2024.

The OMB Draft describes a federal Zero Trust architecture that:

i. Bolsters identity practices.

ii. Relies on encryption and application testing instead of perimeter security.

iii. Recognizes every device and resource the government has.

iv. Supports intelligent automation of security actions.

v. Enables safe and robust use of cloud services.[1]

These goals are organized according to the principals laid out in CISA's Zero Trust Maturity Model, developed to assist agencies as they implement the federal strategy. CISA's model "compliments the OMB's Federal Zero Trust Strategy and is designed to provide agencies with a roadmap and resources to achieve an optimal zero trust environment."[2] The goals involve achievements in identity management, device management, network security, application policy and data protection.[3] Agencies will have 60 days from the OMB Draft's publication to submit their implementation plan for these goals to OMB, along with a budget estimate, and 30 days to designate a lead to coordinate the effort.

What Would the OMB Draft Require for Government Contractors?

Although the proposed OMB Draft applies to federal agencies, it has significant implications for government contractors. The OMB Draft was preceded by President Biden's May 2021 EO 14208, which mandated rapid development of plans by every federal agency for modernizing their approach to cybersecurity, including implementation of Zero Trust architecture. Thus, Zero Trust architecture should be built into any software the federal government acquires or that its contractors use. This approach has been gaining momentum throughout industries that service government contracts, and last year many of the submissions for the Department of Defense mandated Zero Trust architecture in order to qualify for the bid. The Zero Trust framework is consistent with prior Defense Federal Acquisition Regulation Supplement (DFARS) mandates to protect Controlled Unclassified Information (CUI), such as DFARS 252.204-7012, NIST 800-171, ITAR 120.54, and CMMC Level 3.

While not a complete cybersecurity strategy, the OMB Draft provides a roadmap federal agencies can use to form a foundational cyber defense, which can be added to over time. This represents a turn toward a more adaptive view of cyber defense by the federal government, built upon proven methods like Zero Trust architecture, of which CISA's model provides examples. This is an especially encouraging development for businesses that may have harbored doubts about the federal government's commitment to adaptability in the face of cybersecurity's ever-evolving landscape.

We will continue to cover updates to federal cybersecurity policy. The comment period for the OMB Federal Zero Trust Strategy draft ends September 21, 2021, while the comment period for CISA's Zero Trust Maturity Model ends October 1, 2021. If you have any questions, please contact a member of the Akin Gump cybersecurity, privacy and data protection team.

[1] Office of Management and Budget, *Moving the U.S. Government Towards Zero Trust Cybersecurity Principles*, Draft for Public Comment (September 7, 2021) (hereinafter “OMB draft”) available at https://zerotrust.cyber.gov/downloads/Office%20of%20Management%20and%20Budget%20-%20Federal%20Zero%20Trust%20Strategy%20-%20DRAFT%20For%20Public%20Comment%20-%202021-09-07.pdf.

[2] Cybersecurity and Infrastructure Agency, Moving the U.S. Government towards Zero Trust Cybersecurity Principles, Zero Trust Maturity Model (September 7, 2021) available at https://zerotrust.cyber.gov/zero-trust-maturity-model/.

[3] OMB draft at 4.

Categories

Cybersecurity & Information Security

Government Contracts

Attorney advertising. This document is distributed for informational use only; it does not constitute legal advice and should not be used as such. Prior results do not guarantee a similar outcome. Akin is the practicing name of Akin Gump LLP, a New York limited liability partnership authorized and regulated by the Solicitors Regulation Authority under number 267321. A list of the partners is available for inspection at Eighth Floor, Ten Bishops Square, London E1 6EG. For more information about Akin Gump LLP, Akin Gump Strauss Hauer & Feld LLP and other associated entities under which the Akin Gump network operates worldwide, please see our Legal Notices page.