carahsoft.
TECHNOLOGY BY POLICY

Executive Order 14028

Improving the Nation's Cybersecurity

May 12, 2021

Overview

Signed on May 12, 2021, Executive Order 14028: Improving the Nation's Cybersecurity, remains one the federal government's primary framework for strengthening cybersecurity across agencies. Although refined on June 6, 2025, through Executive Order 14306: Sustaining Select Efforts to Strengthen the Nation's Cybersecurity, its core mandates remain firmly in place. The 2025 amendments streamlined overlapping directives and removed redundant software attestation and reporting requirements introduced under Executive Order (EO) 14144, while preserving EO 14028's central focus on **Zero Trust Architecture, secure software development,** and **real-time threat sharing**.

EO 14028 continues to guide federal cybersecurity strategy through **OMB M-22-09** and **CISA's Zero Trust Maturity Model v2.0**. These frameworks ensure that agencies maintain strong identity management, encryption, and continuous verification practices, cementing EO 14028's role as the enduring foundation of the nation's cybersecurity modernization and resilience efforts.

Framework

EO 14028 aims to modernize federal cybersecurity through **secure-by-design development**, **identity modernization**, and **technology innovation**. Additionally, the order authorizes **CISA** to expand real-time threat detection and use **AI-driven analytics** to strengthen response capabilities.

Following the **June 2025 amendments under EO 14306**, the framework remains in effect with streamlined compliance, removing centralized software attestations, scaling back digital identity mandates, and narrowing sanctions authority to foreign actors. The result is a simplified, innovation-driven cybersecurity framework that sustains EO 14028's core mission of building a secure, resilient, and adaptive federal cyber ecosystem.

What Does This Mean for Government?

Federal agencies face mandates to:

- Accelerate implementation of Zero Trust Architecture across networks and mission systems.
- Adopt and verify secure-by-design software development consistent with NIST's SSDF and CISA guidance.
- Deploy phishing-resistant MFA, centralized identity management, and continuous monitoring as baseline security controls.
- Strengthen incident response coordination and real-time threat sharing with CISA using standardized playbooks and reporting protocols.

The EO reinforces cybersecurity as a core element of federal modernization. While compliance requirements have been streamlined under EO 14306, agencies remain responsible for measurable progress in zero trust adoption, software assurance, and post-quantum readiness, solidifying EO 14028 as a key pillar of federal cyber resilience.

What Does This Mean for Industry?

For technology contractors, integrators, and developers, Executive Order 14028 signals continued demand for secure, compliant, and verifiable cybersecurity solutions across the federal enterprise.

Key takeaways for vendors:

- Agencies will prioritize vendors that align with **secure-by-design** principles and can demonstrate compliance with **NIST's Secure Software Development Framework (SSDF)**.
- Solutions that enable or enhance **Zero Trust Architecture**, **phishing-resistant MFA**, and **continuous monitoring** will remain high-value procurement targets.

- Contractors must maintain **attestation-ready documentation** and integrate **AI-driven analytics** and **post-quantum readiness** into product roadmaps to stay competitive.
- Streamlined compliance under **EO 14306** allows vendors to focus less on redundant reporting and more on delivering **innovative, verifiably secure technologies** that strengthen federal resilience.

Timeline

Provisions	Description
Zero Trust Architecture/ Modernization	• Directs all federal agencies to modernize cybersecurity postures using Zero Trust principles ("never trust, always verify"). • Shifts from perimeter-based defenses to continuous, identity- and device-centric validation.
Identity & Access Management /MFA	• Requires deployment of **phishing-resistant multi-factor authentication (MFA)** across all federal systems. • Establishes centralized identity and access management with continuous verification of users and devices.
Threat Sharing & Coordination	• Mandates **real-time cyber threat intelligence sharing** across federal agencies and with industry partners. • Directs **CISA** and **DoD** to coordinate joint defensive operations and information exchanges. • Implemented through the **Joint Cyber Defense Collaborative (JCDC)** and interagency data-sharing protocols.
Software Supply Chain Security	• Requires vendors to follow **secure development practices** aligned with **NIST SP 800-218 (SSDF)**. • Directs agencies to obtain **security attestations** or **software bills of materials (SBOMs)** for all procured software. • Although EO 14144 and EO 14306 simplified attestation methods, the core mandate for verifiable, secure software remains fully active.
Incident Response & Reporting	• Establishes standardized **incident response playbooks** across agencies. • Expands **vulnerability disclosure programs (VDPs)** to encourage public reporting of flaws. • Requires immediate notification to **CISA** for major cyber incidents.

Contact Us:

Email: Research@carahsoft.com

See more from the Carahsoft Team:
To explore our catalog of federal, state, and local technology policies, executive orders, and directives shaping public sector modernization scan this QR code.