



ACCOUNTABILITY | INTEGRITY | RULE OF LAW

EXECUTIVE ORDER

FEDERAL CYBERSECURITY FORTRESS AND SENSITIVE DATA PROTECTION INITIATIVE

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Purpose and Policy.

Federal information systems contain personnel, national-security, law-enforcement, financial, health, biometric, and operational information whose compromise can endanger individuals and the United States. Executive agencies shall modernize these systems around zero-trust principles, strong cryptography, segmentation, resilient storage, continuous monitoring, and rapid containment rather than reliance on a single network perimeter.

Sec. 2. Federal High-Value Data Inventory.

Within 30 days, the Director of the Office of Management and Budget (OMB), in coordination with the Director of the Cybersecurity and Infrastructure Security Agency (CISA), the National Cyber Director, and agency heads, shall establish criteria for Federal High-Value Data Systems. Within 60 days, each agency shall identify systems containing its most sensitive information and submit an appropriately protected inventory.

Sec. 3. Segmented Secure Architecture.

Agencies shall develop migration plans that separate High-Value Data Systems from ordinary enterprise networks through multiple independent security boundaries, least-privilege access, microsegmentation, strong identity and device authentication, application-level controls, and tightly controlled administrative pathways. No system shall be treated as secure merely because it is behind a firewall.

Sec. 4. Encryption and Key Protection.

High-Value Data Systems shall employ strong standards-based encryption for data at rest and in transit, consistent with National Institute of Standards and Technology guidance and applicable national-security requirements. Cryptographic keys shall use approved hardware-backed key management or equivalent controls, separation of duties, rotation, recovery procedures, and auditable access.

Sec. 5. Privileged Access and Zero Trust.

Agencies shall eliminate standing privileged access wherever operationally practicable. Administrative access shall require phishing-resistant multifactor authentication, least privilege, time-limited elevation where feasible, secure administrative workstations, comprehensive logging, and rapid revocation. Access decisions shall continuously evaluate user, device, application, data, and risk context.

Sec. 6. New Secure Hosting Environment.

Within 120 days, OMB, CISA, and the General Services Administration, in consultation with the Department of Defense and other appropriate agencies, shall present an implementation plan for a modern, highly resilient hosting environment for High-Value Data Systems. The plan shall compare dedicated government facilities, approved cloud environments, hybrid architectures, and physically or logically isolated enclaves. Migration shall occur only after security testing, data-integrity validation, continuity planning, and authorization.

Sec. 7. Data Minimization and Compartmentalization.

Agencies shall determine whether sensitive information is being collected, retained, replicated, or made accessible beyond operational necessity. High-Value Data shall be compartmentalized so that compromise of one account, application, network segment, database, or facility does not automatically expose an entire government-wide dataset.

Sec. 8. Immutable and Offline Recovery.

Each High-Value Data System shall maintain tested recovery capabilities, including encrypted backups and, where appropriate, offline or immutable copies protected from alteration by compromised production credentials. Agencies shall conduct recurring restoration exercises.

Sec. 9. Continuous Detection, Logging, and Threat Hunting.

Agencies shall maintain centralized tamper-resistant security logging, continuous monitoring, endpoint detection and response, network and identity telemetry, and threat-hunting capabilities appropriate to system risk. Critical alerts shall be triaged continuously. CISA shall establish minimum logging and retention requirements for civilian executive agencies consistent with law and OMB policy.

Sec. 10. Independent Red-Team Testing.

High-Value Data Systems shall undergo recurring independent penetration testing, red-team exercises, vulnerability assessments, and configuration reviews under controlled authorization. Testing shall include identity compromise, lateral movement, data exfiltration, supply-chain, recovery, and insider-risk scenarios without unnecessarily exposing operational vulnerabilities.

Sec. 11. Legacy-System Replacement.

Within 180 days, each agency shall identify unsupported, end-of-life, or materially insecure hardware and software supporting High-Value Data Systems and submit a prioritized replacement schedule to OMB. OMB shall identify funding, acquisition, workforce, and statutory barriers and recommend budgetary or legislative action where required.

Sec. 12. Software and Supply-Chain Security.

Agencies shall strengthen software supply-chain controls for High-Value Data Systems, including secure development practices, vulnerability remediation, software inventory, provenance and integrity verification, contractor security requirements, and risk-based restrictions on components presenting unacceptable national-security risk.

Sec. 13. Incident Containment and Notification.

Agencies shall maintain rehearsed incident-response plans capable of rapidly isolating compromised identities, endpoints, network segments, applications, and data stores. CISA and OMB shall establish government-wide escalation requirements for significant civilian-agency incidents, consistent with statutory reporting obligations.

Sec. 14. Office of Personnel Management Priority Review.

Because the Office of Personnel Management experienced major breaches in 2015 affecting personnel and background-investigation information, OPM shall receive priority review. Within 90 days, OPM, OMB, and CISA shall assess the security architecture of OPM High-Value Data Systems, applicable open cybersecurity recommendations, logging, privileged access, segmentation, backup resilience, and modernization needs and establish corrective milestones.

Sec. 15. Accountability Dashboard.

OMB and CISA shall maintain an executive cybersecurity accountability process identifying overdue critical remediation items, responsible agency leadership, target completion dates, accepted risks, and resource constraints. Sensitive vulnerability details shall not be publicly disclosed. Aggregate progress shall be reported publicly to the extent consistent with national security and law.

Sec. 16. Cybersecurity Workforce.

OPM, CISA, and agency heads shall identify critical cybersecurity staffing shortages and propose accelerated lawful hiring, retention, training, and specialized career pathways. Agencies shall ensure personnel assigned to sensitive systems possess appropriate qualifications and recurring security training.

Sec. 17. Ninety-Day Presidential Report.

Within 90 days, OMB, CISA, and the Office of the National Cyber Director shall submit a consolidated report to the President identifying the highest-priority modernization actions, immediate vulnerabilities requiring remediation, estimated costs, implementation timelines, and any legislative authorities or appropriations needed from Congress.

Sec. 18. General Provisions.

(a) This order shall be implemented consistent with applicable law and statutory responsibilities assigned to agency heads and independent agencies.

(b) Nothing in this order authorizes access to information otherwise prohibited by law, weakens privacy protections, or supersedes lawful classification and intelligence-community requirements.

(c) Nothing in this order shall be construed to guarantee that any information system is impenetrable. Agencies shall instead employ defense-in-depth, resilience, continuous verification, and rapid recovery to reduce the probability and consequences of compromise.

(d) Implementation is subject to the availability of appropriations.

(e) This order creates no right or benefit enforceable at law or in equity against the United States, its agencies, officers, employees, or any other person.

THE PRESIDENT

THE WHITE HOUSE,
_____, 20__.

DRAFTING NOTE

This proposal uses defense-in-depth and zero-trust architecture rather than promising an 'impenetrable' network. It directs modernization, segmentation, encryption, resilient storage, continuous monitoring, independent testing, and priority remediation while preserving statutory authorities and congressional control of appropriations.