Kiteworks

GUIDE

How Federal Agencies Can Comply With the Data Requirement in Executive Order 14028

Building on Executive Order 14028 To Improve the Nation's Cybersecurity

In response to cyberattacks becoming increasingly more complex over the past couple years, the U.S. White House issued an Executive Order (EO 14028) in May 2021—*Improving the Nation's Cybersecurity*—requiring federal agencies to ask their suppliers to provide software bill of materials (SBOMs). Further clarification was provided in September 2021 when the Office of Management and Budget (OMB) and the Cybersecurity and Infrastructure Security Agency (CISA) released three draft guidance documents on a zero-trust strategy.

Additional detail was added to the draft documents from September with the release of a new memorandum from the White House on January 26, 2022. The premise of the memorandum is that perimeter-based security defenses are no longer sufficient to protect critical systems and data. The actions spelled out in the memorandum are meant to help agencies accelerate their transition to zero trust. The premise of a zero-trust model is that "no actor, system, network, or service operating outside or within the security perimeter is trusted." Federal agencies must move from a verify-once-at-the-perimeter cybersecurity approach to continual verification of each user, device, application, and transaction.[1]

Tracking and Controlling Sensitive Data

Governance and protection of sensitive content is referenced throughout the almost 30-page memorandum. The zero-trust strategy depicted therein assumes that agency systems are isolated from each other, and that network traffic flowing between and within them is reliably encrypted. The latter includes the direction that all data must be encrypted while in transit. The memorandum also assumes that security and data teams will work together "to develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information."

As part of the above process, the memorandum calls on security and data teams within and across federal agencies to categorize data based on protection needs—ultimately building a foundation to automatic security access rules. Further, access is based not only on who or what is accessing data but on the sensitivity of the data itself.

"Tightening access controls will require agencies to leverage data from different sources to make intelligent decisions, such as analyzing device and user information to assess the security posture of all activity on agency systems."[2]

A critical starting point in protecting data requires centralized identity management systems that employ multi-factor authentication for staff, contractors, and partners. Multi-factor authentication must be applied at the application layer, not through network authentication. For sensitive content sent via email, encryption is mandated in the memorandum. Email encryption is particularly important for communications sent to third parties. Per the memorandum, "It remains challenging today to easily and reliably encrypt an email all of the way between any sender and any recipient. Unlike HTTP and DNS, there is not today a clear path forward guaranteeing that Federal emails are encrypted in transit, particularly for emails with external parties."[3]

Federal agencies are required to achieve specific zero-trust security goals by the end of fiscal year 2024. These goals encompass five areas with data as the fifth one (the other four are identity, devices, networks, and applications and workloads). Actions are broken into four categories (Table 1). The task mandate in the memorandum for data is to complete the following within 120 days:

Action Stipulated	
Develop Data Security Strategy	Federal Chief Data Officers and Chief Information Security Officers will create a joint committee to develop a zero-trust data security guide for agencies.
Automate Security Responses	Agencies must implement initial automation of data categorization and security responses, focusing on tagging and managing access to sensitive documents.
Audit Access to Sensitive Data	Agencies must audit access to any data encrypted at rest in commercial cloud infrastructure.
Govern Logging and Information Sharing	Agencies must work with CISA to implement comprehensive logging and information-sharing capabilities, as described in OMB Memorandum M-21-31.[4]

Table 1. Actions stipulated in the January 26, 2022, memorandum around data.

"Agency Chief Data Officers must work with key agency stakeholders to develop a set of initial categorizations for sensitive electronic documents within their enterprise, with the goal of automatically monitoring and potentially restricting how these documents are shared."[5]

The memorandum spells out four specific actions when it comes to data:

1. Develop a Data Security Strategy

While agencies inventory their datasets today, this does not comply with the requirements of a zero-trust approach. Part of the challenge is that data is loosely structured and dispersed and intermediate datasets exist principally to support the maintenance of other primary datasets. To address this issue, the memorandum authorizes the formation of a working group led by the OMB consisting of members from the Federal Chief Data Officer Council and the Federal Chief Information Security Officer Council. The working group will develop enterprise-specific data categories that are not addressed by existing federal categories.

2. Automate Security Responses

Automation of security monitoring and enforcement is a critical requirement throughout on-premises systems and cloud infrastructure. One objective of this directive is to avoid disruption to the daily work of users. Data categorization is to include the types of data being protected and who is accessing the data. Within 120 days of issuance of the memorandum, data categorizations need to be delineated; while they do not need "to be complete, they should be broad enough to be useful while being specific enough to be reliably accurate." In accordance with the memorandum, agencies are to automate the restriction of permissions for reviewing and sending sensitive content.

3. Audit Access to Sensitive Data

Organizations are directed in EO 14028 to use encryption to protect data at rest. Per the memorandum, keys can be customer-managed or provider-managed, but for key management, any decryption attempts must be reliably logged by a separate system. The memorandum recommends that audit logs be combined with other sources of event data for more sophisticated approaches to security monitoring.

4. Govern Access to Logging and Information Security

The cybersecurity memorandum from last summer requires centralized access and visibility of information-sharing between agencies for the highest-level security operations center (SOC) of each agency.[6] The objective is to accelerate incident response and investigative efforts. Included among the priorities is the need to implement integrity measures limiting access to and allowing cryptographic verification of logs and logging DNS requests made throughout their environment.

Using Kiteworks To Meet Memorandum Data Requirements

Kiteworks' mission is to protect privacy and ensure compliance of all sensitive content sent via email, file share, automated file transfer, application programming interface (API), and web form through one platform. For federal agencies, they can unify, track, control, and secure sensitive content as it moves within, into, and out of their organizations using the Kiteworks platform. This continuous governance and security approach complies with zero-trust principles spelled out in the memorandum. Table 2 delineates how Kiteworks enables federal agencies to satisfy data-related requirements quickly and easily in the memorandum.

Kiteworks uses a defense-in-depth approach that includes a hardened appliance with all unnecessary services disabled, encryption in transit and at rest, FIPS 140-2 validation, built-in network and web application firewalls (WAFs), continuous data protection capabilities, antivirus, and integration with data loss prevention and advanced threat protection. It also uses key encryption hardening such as storing keys in a Keychain/Keystore wrapper and assigning each volume its own set of keys. Kiteworks assume-breach architecture is also based on zero trust that slows attackers and rapidly alerts security operations teams when an attack occurs.

Actions Related to Data	How Kiteworks Addresses It
Encrypt Email	Secure all inbound and outbound email communications using email encryption gateway. Enforce geofencing by setting block-lists and allow-lists for IP address ranges. Users send emails with sensitive content from any location or device with enterprise-grade encryption and automated security and compliance controls.
Automate Data Categorization	Set automated policies for content sharing based on who is sending to whom, when it was sent, what device was used, how it was accessed, as well as classification metadata such as Microsoft Information Protection (MIP) tags. Kiteworks includes detailed metadata about the user, device, storage, and more regardless of whether the agency deploys on-premises, on IaaS, PaaS (Kiteworks hosted), or FedRAMP.
Audit Access to Sensitive Data	Normalize logging across all communication channels and generate alerts and detailed reports. Includes a CISO dashboard with complete visibility to all information exchanged across the Kiteworks platform.
Monitor Risk Continuously	Dynamically track the inventory of digital assets in motion, visualize all information entering and leaving the agency, and detect suspicious activity and act on anomalies in real time. Includes ability to forward pre-correlated real-time feeds into the SIEM.
Use Multi-factor Authentication and SSO	Kiteworks supports SAML 2.0 and Kerberos and integrates with LDAP and Active Directory across all content communication channels. In addition, Kiteworks supports multiple 2FA options, including OTP via email, text message, Google/Microsoft Authenticator, and any Radius Protocol-based options.

Table 2. Mapping Kiteworks capabilities to memorandum actions.

Kiteworks is already compliant with various federal standards, including the Cybersecurity Maturity Model Certification (CMMC), SOC 2, the Federal Information Security Management Act (FISMA), and FIPS 140-2. Kiteworks also has FedRAMP authorization for Moderate Impact Level Information and satisfies requirements for the General Data Protection Regulation (GDPR), International Traffic in Arms Regulations (ITAR), and the National Institute of Standards and Technology (NIST) 800-171.

Governing and Protecting Sensitive Content Communications

The process of attaining zero trust will be a journey for federal agencies. Solutions that shift security from the network perimeter to continuous monitoring of infrastructure, applications, and data will be key enablers of this transition.

The sharing of data within and between agencies and with third parties creates both opportunity and risk. Regardless of the communication channel used, Kiteworks provides a private content network for this information sharing. Its platform approach unifies tracking and controls while its comprehensive security architecture and capabilities align with core zero-trust principles. For federal agencies seeking to comply with actions around data communications in the latest White House memorandum, Kiteworks offers a comprehensive solution.

[1] "Memorandum: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," Office of Management and Budget, January 26, 2022.

[2] Ibid.

[3] Ibid.

[4] "Memorandum: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," Office of Management and Budget, August 27, 2021.

[5] "Memorandum: Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," Office of Management and Budget, January 26, 2022.

[6] "Memorandum: Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," Office of Management and Budget, August 27, 2021.