



# SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS

## E.O. 14117 Implementation

DEFEND TODAY,  
SECURE TOMORROW

JANUARY 2025

## SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS

### Pursuant To Exec. Order 14117, *Preventing Access To Americans' Bulk Sensitive Personal Data And United States Government-Related Data By Countries Of Concern*

On February 28, 2024, President Biden signed Executive Order (E.O.) 14117, *Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern*, to address national-security and foreign-policy threats that arise when countries of concern and covered persons can access bulk U.S. sensitive personal data or government-related data that may be implicated by the categories of restricted transactions.

As directed by E.O. 14117, CISA has developed the following security requirements to apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). See *generally* 28 C.F.R. part 202 (identifying classes of restricted transactions at 28 C.F.R. § 202.401).

### BACKGROUND

The security requirements are designed to mitigate the risk of sharing U.S. government-related data or bulk U.S. sensitive personal data with countries of concern or covered persons through restricted transactions.<sup>1</sup> They do this by imposing conditions specifically on the covered data, as defined below, that may be accessed as part of a restricted transaction; on the covered systems, as defined below, more broadly; and on the organization as a whole. While the requirements on covered systems and on an organization's governance of those systems apply more broadly than to the data at issue and the restricted transaction itself, CISA assesses that implementation of these requirements is necessary to validate that the organization has the technical capability and sufficient governance structure to appropriately select, successfully implement, and continue to apply the covered data-level security requirements in a way that addresses the risks identified by DOJ for the restricted transactions. For example, to ensure and validate that a covered system denies covered persons access to covered data, it is necessary to maintain audit logs of such accesses as well as organizational processes to utilize those logs. Similarly, it is necessary for an organization to develop identity management processes and systems to establish an understanding of what persons may have access to different data sets.

In addition to requirements on covered systems, applying security requirements on the covered data itself that may be accessed in a restricted transaction is also necessary to address the risks. The specific requirements that are most technologically and logistically appropriate for different types of restricted transactions may vary. For example, some transactions may be amenable to approaches that minimize data or process it in such a way that does not reveal covered data to covered persons. In other cases, techniques such as access control and encryption may be more appropriate to deny any access by covered persons to covered data. The security requirements contemplate multiple options to minimize the risk to covered data, though all of the options build upon the foundation of the requirements imposed on covered systems and the organization as a whole. While U.S. persons engaging in restricted transactions must implement all of the organizational- and covered-system level requirements, such persons will have some flexibility in determining which

<sup>1</sup> CISA notes that these security requirements are, as required by the E.O., designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." E.O. 14117 Sec. 2(d). They are not intended to reflect a comprehensive cybersecurity program. For example, several areas addressed in CISA's Cross-Sector Cybersecurity Performance Goals (CPGs), available at <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>, are not reflected in the data security requirements, even though the CPGs themselves are a common set of protections that CISA recommends all critical infrastructure entities voluntarily implement to meaningfully reduce the likelihood and impact of known risks and adversary techniques. As the operational lead for federal cybersecurity and national coordinator for critical infrastructure security and resilience, CISA recommends that all U.S. persons implement cybersecurity best practices in light of the risk and potential consequence of cyber incidents.

combination of data-level requirements is sufficient to address the risks posed, based on the nature of the transaction, so long as the combination of security mechanisms deployed fully and effectively prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern. If a combination of security mechanisms proves to be insufficient to prevent such access, that combination of security mechanisms will be considered invalid in protecting future access to covered data by covered persons.

## IN GENERAL

The security requirements provide the organizational- and covered system-level requirements (Section I) and covered data-level requirements (Section II) which U.S. persons engaging in restricted transactions must meet. These security requirements are in addition to any compliance-related conditions imposed in applicable DOJ regulations. See 28 C.F.R. § 202.1001–202.1201. References below to the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF),<sup>2</sup> NIST Privacy Framework (PF),<sup>3</sup> and CISA’s Cross-Sector Cybersecurity Performance Goals (CPGs)<sup>4</sup> are intended to help the reader understand which aspects of existing frameworks, guidance, or other resources these security requirements are based upon, consistent with the requirements of the E.O. Understanding and applying these security requirements does not require a reader to also understand and apply the referenced resources.

## DEFINITIONS

To the extent these security requirements use a term already defined in DOJ’s regulation, see 28 C.F.R. § 202.201-202.259, CISA’s use of that term below carries the same meaning.

For the purpose of these security requirements:

- **Asset** means data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes.
- **Covered data** means government-related data bulk U.S. sensitive personal data.
- **Covered system:**
  - means an information system used to obtain, read, copy, decrypt, edit, divert, release, affect, alter the state of, view, receive, collect, process, maintain, use, share, disseminate, or dispose of (collectively, “interact with”) covered data as part of a restricted transaction, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified; and
  - does not include an information system (e.g., an end user workstation) that has the ability to view or read sensitive personal data (other than sensitive personal data that constitutes government-related data) but does not ordinarily interact with such data in bulk form.<sup>5</sup>
- **Information system** means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- **Network** means a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

<sup>2</sup> NIST, Cybersecurity Framework ver. 2.0, available at <https://www.nist.gov/cyberframework>.

<sup>3</sup> NIST, Privacy Framework ver. 1.0, available at <https://www.nist.gov/privacy-framework>.

<sup>4</sup> CISA, Cross-Sector Cybersecurity Performance Goals, available at <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.

<sup>5</sup> For example, if an end user workstation only interacts with individual records of U.S. sensitive personal data, although it may have the ability to “read” or “view” bulk U.S. sensitive personal data, it is not deemed on its own to be a covered system unless it takes further actions outlined in the definition of covered system (e.g., maintaining or processing data in excess of the bulk thresholds) with respect to such data. Note that there are no bulk thresholds for government-related data and individual records would be considered covered data. Thus, end user workstations that interact with government related data are covered systems.

## SECURITY REQUIREMENTS

- I. **Organizational- and System-Level Requirements.** For any covered system:
  - A. Ensure basic organizational cybersecurity policies, practices, and requirements, including all of the following, are in place:
    1. Identify, prioritize, document all assets of the covered system.
      - a. Maintain, to the maximum extent practicable, an updated inventory of covered system assets with each system's respective internet protocol (IP) address (including IPv6).<sup>6</sup> (NIST CSF 2.0 ID.AM-01, CISA CPGs 1.A)
      - b. Ensure inventory is updated on a recurring basis, no less than monthly for Information Technology (IT) assets. (NIST CSF 2.0 ID.AM-08, CISA CPGs 1.A)
    2. Designate, at an organizational level, an individual (e.g., a Chief Information Security Officer) responsible and accountable for (1) cybersecurity and (2) governance, risk, and compliance functions (GRC). This could be one individual responsible and accountable for both areas, or one individual for each of these two areas. (NIST CSF 2.0 GV.RR-02, CISA CPGs 1.B)
    3. Remediate known exploited vulnerabilities (KEVs) in internet-facing systems within a risk-informed span of time, prioritizing the most critical assets first and completing remediation for all such vulnerabilities within 45 calendar days. (NIST CSF 2.0 ID.RA-01 and 08 CISA CPGs 1.E)
      - a. Implement alternative compensating requirements, should patching not be feasible.
      - b. Establish a process to evaluate, after patching, whether internet-facing covered systems with KEVs were compromised prior to patching.
    4. Document and maintain all vendor/supplier agreements for covered systems (e.g., third-party network connection agreements), including contractual IT and cybersecurity requirements. (NIST CSF 2.0 GV.SC-05, 06, 07, 10, CISA CPGs 1.G, 1.H, 1.I)
    5. Develop and maintain an accurate network topology of the covered system and, to the extent technically feasible, any network interfacing with a covered system to facilitate visibility into connections between assets, and aid in timely identification of and response to incidents. (NIST CSF 2.0 ID.AM-03, CISA CPGs 2.P)
    6. Adopt and implement an administrative policy that requires approval before new hardware or software is deployed in/on a covered system. U.S. persons engaging in restricted transactions must maintain a risk-informed allowlist of approved hardware and software for covered systems. (NIST CSF 2.0 GV.PO-02, ID.RA-09, ID.AM-08, PR.PS-01, 02, 03, CISA CPGs 2.Q)
    7. Develop and maintain incident response plan(s) applicable to covered systems, which should be reviewed annually and updated as appropriate. (NIST CSF 2.0 ID.IM-04, CISA CPGs 2.S, 5.A)
  - B. Implement logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data that does not comply with the data-level requirements (Section II) including through information systems, cloud-computing platforms, networks, security systems, equipment, or software. (NIST CSF 2.0 PR.AA-01 through PR.AA-06) Specifically, U.S. persons engaging

<sup>6</sup> This list may be maintained in an automated fashion that tracks dynamic changes in the covered system (e.g., automatic provisioning of virtual machines or containers in a cloud environment) and may consist of several constituent parts for discrete subsystems.

in restricted transactions must:

1. Enforce multifactor authentication (MFA) on all covered systems (e.g., by requiring an Authentication Assurance Level (AAL) AAL2 or AAL3 authenticator as defined in the most recent version of NIST Special Publication 800-63B and/or its supplements), or in instances where MFA is not technically feasible and/or not enforced, require passwords have sufficient strength, including sufficient length of 15 or more characters. (NIST CSF 2.0 PR.AA-03, PR.AA-04, CISA CPGs 2.B, 2.H)
  2. Promptly revoke (e.g., on day of departure or within a risk-informed timeframe) any individual credentials, shared credentials, and/or authorized access to covered systems upon termination or change in roles for any individual with access to covered system(s). (NIST CSF 2.0 GV.RR-04, PR.AA-01, & PR.AA-04, CISA CPGs 2.D)
  3. Collect logs for covered systems pertaining to access- and security-focused events (e.g., intrusion detection systems/intrusion prevention systems, firewall, data loss prevention, virtual private network, and detection of unsuccessful login events), and store such logs for use in both detection and incident response activities (e.g., forensics to assist in detection, response, and recovery). Implement a process to notify cybersecurity personnel when a critical log source, such as an operating system event logging tool, is not producing and retaining logs as expected. (NIST CSF 2.0 PR.PS-04, & DE.CM-03, and 09, CISA CPGs 2.T, 2.U)
    - a. Securely store collected logs in a central system, such as a security information and event management tool or central database, for at a minimum 12 months. In the event of a data breach or a violation of these security requirements, logs should be maintained until final resolution of the matter by the U.S. Government.
    - b. Ensure that collected logs may only be accessed or modified by authorized and authenticated users.
  4. Implement configurations to deny by default (e.g., by requiring authentication) all connections to covered systems and any network on which covered systems reside, unless connections are explicitly allowed for specific system functionality. (NIST CSF 2.0 PR.PS-01)
  5. Issue and manage, at an organizational level, identities and credentials for authorized users, services, and hardware, with sufficient attributes available to prevent access by covered persons or countries of concern to covered data that does not comply with the data-level requirements (Section II). Limit system access to the types of transactions and functions that authorized users are permitted to execute. (NIST CSF 2.0 PR.AA-05, CISA CPGs 2.C)
- C. Conduct an internal data risk assessment that evaluates whether and how the overall approach selected and implemented pursuant to Section II sufficiently prevents access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, taking into consideration the likelihood of disclosure and the likelihood of harm based on the nature of the transaction and the data at issue, to include potential data misuse and associated consequences. The risk assessment must include a mitigation strategy outlining how implementation will prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern. The risk assessment should be reviewed annually by the organization and updated as appropriate. (NIST Privacy Framework ID.RA-P1, NIST Privacy Framework ID.RA-P3, NIST Privacy Framework ID.RA-P4, NIST Privacy Framework ID.RA-P5)

- II. **Data-Level Requirements.** For any restricted transaction, implement a combination of the following mitigations that, taken together, is sufficient to fully and effectively prevent access to covered data that is linkable, identifiable, unencrypted, or decryptable using commonly available technology by covered persons and/or countries of concern, consistent with the data risk assessment described in Section I.C.:
- A. Apply data minimization and data masking strategies to reduce the need to collect, or sufficiently obfuscate, respectively, covered data to prevent visibility into that data, without precluding the U.S. persons engaging in restricted transactions from conducting operations with the data. These strategies must include:
1. Maintaining and implementing a written data retention and deletion policy, to be reviewed annually and updated as appropriate. (*NIST Privacy Framework GV.PO-P1, CT.PO-P2*)
  2. Processing data in such a way to either render it no longer covered data or minimize the linkability to U.S. person entities before it is subject to access by a covered person or country of concern. (*NIST Privacy Framework CT.DP-P2*)
    - a. This may be achieved through application of techniques such as aggregation, pseudonymization, de-identification, or anonymization.
    - b. When implemented, observability and linkability of data must be minimized to ensure U.S. person identities cannot be inferred or extrapolated from the individual data set at issue or in combination with other data sets the recipient or recipient-linked organizations are known to hold.
    - c. Aggregations of covered data must be based on at least the number of records required to render the data “bulk” under the regulations found at 28 C.F.R. § 202.205.
  3. Treating information systems that implement such processing as covered systems subject to the requirements of Section I. (*NIST Privacy Framework CT.DP-P4, CM.AW-P3, GV.PO-P2*)
- B. Apply encryption techniques to protect covered data during the course of restricted transactions. These techniques must include:
1. Comprehensive Encryption: Encrypt covered data in a restricted transaction, regardless of type, during transit and storage.<sup>7</sup> (*NIST Privacy Framework CT.DP-P1, PR.DS-P1, PR.DS-P2, CISA CPGs 2.K*)
  2. Key Management: Generate and securely manage cryptographic keys used to encrypt covered data, including the following practices: (*NIST Privacy Framework CT.DP-P1 & PR.DS-P2, CISA CPGs 2.L*)
    - a. Do not co-locate encryption keys with covered data.
    - b. Do not store encryption keys, via any mechanism (physically or virtually), in a country of concern.
    - c. Covered persons must not be authorized to have access to encryption keys.

<sup>7</sup>For the purposes of this requirement, CISA considers comprehensive encryption to mean cryptographic algorithms, ciphers, and protocols that are ordinarily accepted by U.S. persons with significant expertise in cryptography as being sufficient to provide confidentiality and integrity protections to sensitive data against compromise by currently known techniques and a level of computing power that is reasonably foreseeable to be available to any person, organization, or country in the near future. CISA considers U.S. Government approved encryption algorithms, ciphers, and protocols to meet this standard, but organizations may determine that other algorithms, ciphers, and protocols also qualify. For connections made using Transport Layer Security (TLS), only version 1.2 or higher is considered comprehensive encryption.

- d. All information systems responsible for the storage of and access to encryption keys must be considered covered systems subject to the requirements of Section I.
- C. Apply privacy enhancing technologies, such as privacy preserving computation (e.g., homomorphic encryption), or differential privacy techniques (e.g., inject sufficient noise into processing of data to preclude the reconstruction of covered data from the processed data), to process covered data. Use of such techniques are subject to the following:
1. The application of privacy enhancing technologies must not reveal to covered persons participating in the restricted transaction covered data or information that could reasonably likely be used to reconstruct covered data, including by linking processed data with other data sets (e.g., allowing a covered person to participate in a privacy preserving computation that requires trusted parties would not be permissible).
  2. For the avoidance of doubt, information systems that implement such processing are covered systems subject to the requirements of Section I. (*NIST Privacy Framework CT.DP-P1*)
- D. Configure the previously outlined identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern within all covered systems. (*NIST Privacy Framework PR.AC-P4*)