PREVENTING ACCESS TO US SENSITIVE PERSONAL DATA AND GOV'T RELATED DATA BY COUNTRIES OF CONCERN OR COVERED PERSONS

PROPOSED SECURITY REQUIREMENTS FOR RESTRICTED TRANSACTIONS

Table of Contents

- Background
- Organization- & System-Level Requirements
- Data-Level Requirements

Background

Background

- The security requirements mitigate the risk of sharing bulk U.S. sensitive personal data in restricted transactions
- They impose conditions:
  - On the covered data that may be shared as part of a restricted transaction;
  - On covered systems more broadly; and
  - On the organization as a whole.

– Organization- and system-level requirements: These help 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.

– Data-level requirements: 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 combination of data-level requirements are sufficient to address the risks posed, based on the nature of the transaction, 1 CISA notes that these security requirements are, as required by the E.O., designed to "address the unacceptable risk posed by restricted

Background (cont'd)

- 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 combination of data-level requirements are 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 by covered persons.
- If a combination of security mechanisms proves to be insufficient to prevent access to covered data by covered persons, those security mechanisms will be considered invalid in protecting future access to covered data by covered persons.

Organization- and System-Level Requirements

• Organization- & System-Level Requirements

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 a regularly updated inventory of covered system assets with each system's respective internet protocol (IP) address (including IPv6). For hardware, this should also include MAC address. (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) within 14 calendar days; other vulnerabilities (those not known to be exploited) must be remediated within 15 calendar days if deemed critical severity, or 30 calendar days if deemed high severity. (NIST CSF 2.0 ID.RA-01 and 08 CISA CPGs 1.E)
   a. Should patching not be feasible, alternative compensating requirements must be implemented.
   b. U.S. persons engaging in restricted transactions must document all mitigation measures (patch or compensating requirement) that are implemented.
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 maximum extent practicable, 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 includes a manual or automated process that requires approval before new hardware, firmware, or software/software version is installed or deployed in a covered system. (NIST CSF 2.0 GV.PO-02, ID.RA-09, ID.AM-08, PR.PS-01, 02, 03, CISA CPGs 2.Q)
   a. U.S. persons engaging in restricted transactions must maintain a risk-informed allowlist of approved hardware, firmware, and software for covered systems.
   b. The risk-informed allowlist must include specification of approved versions, for covered systems.
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)

• Organization- & System-Level Requirements (cont'd)

Implement logical and physical access controls to prevent covered persons or countries of concern from gaining access to covered data, in any form, including through information systems, cloud-computing platforms, networks, security systems, equipment, or software. (NIST CSF 2.0 PR.AA-01 through PR.AA06) Specifically, U.S. persons engaging in restricted transactions must:

1. Enforce multifactor authentication (MFA) on all covered systems, or in instances where MFA is not feasible, require passwords have sufficient strength, including sufficient length of 16 or more characters. (NIST CSF 2.0 PR.AA-03, PR.AA-04, CISA CPGs 2.B, 2.H)
2. Immediately revoke, upon termination or change in roles for any individual with authorized access to covered system(s), any credentials assigned to that individual. (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). Notify cybersecurity personnel when a critical log source, such as an operating system event logging tool, is disabled. (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. Maintain organizational policies and processes to ensure that unauthorized media and hardware are not connected to covered assets, such as by limiting use of Universal Serial Bus (USB) devices and removable media or disabling AutoRun. (NIST CSF 2.0 PR.DS-01, PR.AA-06, & GV.PO-01, CISA CPGs 2.V)
5. Implement configurations to deny by default 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)
6. Issue and manage, at an organizational level, identities and credentials for authorized users, services, and hardware, with sufficient attributes available to prevent access of covered data by covered persons or countries of concern. 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)

Organization- & System-Level Requirements (cont'd)

- Conduct and document a data risk assessment that evaluates whether and how the overall approach selected and implemented pursuant to section II sufficiently prevents access to covered data 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 shall include a mitigation strategy outlining how implementation will prevent access to covered data by covered persons and/or countries of concern.
- The risk assessment should be reviewed annually 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

Data-Level Requirements

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 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 shall 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. Information systems that implement such processing are 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 using industry-standard encryption. (NIST Privacy Framework CT.DP-P1, PR.DS-P1, PR.DS-P2, CISA CPGs 2.K)
   2. Transport Layer Security (TLS): Transmit covered data in a restricted transaction over the Internet only using Transport Security Layer (TLS) 1.2 or higher protocols. (NIST Privacy Framework CT.DP-P1 & PR.DS-P2, CISA CPGs 2.K)

• Data-Level Requirements (cont'd)

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 by covered persons and/or countries of concern, consistent with the data risk assessment described in section I.C (cont'd):

1. 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 shall not be authorized to have access to encryption keys.
   d. All information systems responsible for the storage of and access to encryption keys shall 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 shall 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)

GLOBAL DATA ALLIANCE

TRUST ACROSS BORDERS

Please direct any questions to gdainfo@bsa.org