Updates
December 03, 2024
CISA Security Requirements for Restricted Data Transactions Under New DOJ Rule

President Joe Biden issued Executive Order (EO) 14117 in February 2024 to mitigate national security risks posed by threat countries' access to sensitive personal data and government-related data. The EO directed the U.S. Department of Justice (DOJ) to issue implementing regulations and directed the U.S. Department of Homeland Security, Cybersecurity and Infrastructure Security Agency (CISA) to develop related security measures for classes of transactions. This Article summarizes CISA's proposed security guidelines for "restricted transactions," subject to the rules DOJ proposed in a Notice of Proposed Rulemaking (NPRM), which is summarized here. DOJ's announced compliance and enforcement approach will be summarized separately.

Background

DOJ's NPRM governs transfers of bulk U.S. person sensitive data and government-related data (covered data). U.S. persons engaging in "restricted transactions" —vendor, employment, and investment agreements that give countries of concern (CoCs) or covered persons (CPs) access to covered data—must apply the CISA security guidelines.

Critically, the systems and organizational requirements applicable to parties that engage in restricted transactions apply more broadly than the data subject to the specific restricted transaction. The CISA security requirements impose conditions at three levels: on the covered data that is subject to a restricted transaction; on "covered systems," which process such data; and on organizations subject to the DOJ rules. The CISA security requirements include governance and organizational components, as well as technical controls. The requirements are based on existing cybersecurity guidance and should look familiar to security professionals.

Proposed Requirements

At the organization and system level, the CISA security requirements direct entities to:

- Implement basic cybersecurity policies, practices, and requirements, including:
    - Maintaining and updating an asset inventory for covered systems.
    - Designating personnel accountable for cybersecurity, governance, risk management, and compliance.
    - Remediating vulnerabilities based on designated timeframes based on level of risk.
    - Documenting vendor and supplier agreements for covered systems.
    - Maintaining accurate network topologies of covered systems and of networks interfacing with covered systems.
    - Implementing policies that require approval for deployment of new hardware, firmware, or software on covered systems.
    - Maintaining, periodically reviewing, and updating incident response plans for covered systems.
- Implement access controls, both logical and physical, to prevent CoCs or CPs from accessing covered data in any form. Specific requirements include:
    - Enforcing multifactor authentication (MFA) on all covered systems.
        - If MFA is not possible, strong passwords of 16 or more characters are required.
    - Immediately revoking access credentials for any user upon termination of that user's authorization to access a covered system.
    - Collecting system logs and securely maintaining logs for 12 months.
    - Employing policies and processes to prevent connection of unauthorized media or hardware to covered systems.
    - Configuring covered systems and networks containing covered systems to deny connections by default.
    - Implementing identity and credential management practices that prevent CoCs and CPs from accessing covered data.
- Conduct and document a risk assessment that evaluates whether data-level security measures prevent CoCs and CPs from accessing covered data. The assessment must be conducted annually.
- At the data level, the CISA security requirements direct entities to implement a combination of listed mitigations that, as a whole, will effectively prevent CoCs and CPs from accessing covered data. The particular combination of measures will depend on the risk assessment described above. Options include the following: Data minimization and masking strategies, which must include:
    - A written data retention and deletion policy.
    - Data processing that eliminates or reduces linkability to U.S. persons before a CoC or CP can access it, such as through aggregation, pseudonymization, de-identification, or anonymization.
        - This processing must minimize observability and linkability of data to prevent CoCs and CPs from inferring or extrapolating U.S. person identities.
- Specific encryption to protect covered data during restricted transactions, which must include:
    - Comprehensive encryption (*i.e.*, encryption during transit and in storage).
    - Transport layer security for covered data transmitted over the internet in a restricted transaction.
    - Proper cryptographic key management.
        - Keys may not be stored in a CoC, and CPs must not have access to keys.
- Application of privacy-enhancing technologies, such as:
    - Homomorphic encryption, which allows computation without decryption.
    - Differential privacy, such as adding "noise" to obfuscate covered data.
- Configuring identity and access management measures to prevent CoCs and CPs from having authorized access to covered data.

Note that several measures, such as encryption, pseudonymization, and anonymization, are available as mitigation measures, even though their application is *not* sufficient to exempt otherwise covered data from the NPRM itself.

The security guidelines provide additional specifications for the measures described above. They also cross-reference industry standards, including the National Institute of Standards and Technology's (NIST) Privacy Framework and Security Framework and CISA's Cybersecurity Performance Goals.

CISA Questions for the Public

Public comment is welcome on any topic, but CISA seeks input on the following, in particular:

1. The sufficiency of the proposed requirements.
2. Whether the higher-level requirements are sufficient to ensure proper limitations on access to covered data.
3. Whether the security requirements are overly burdensome and/or appropriately detailed.
4. For the data-level requirements:
    1. Whether additional requirements should be considered to permit commercial transactions while protecting covered data.
    2. Whether any specific requirements should be mandatory, regardless of an individual risk assessment.
    3. Whether additional guidance should be issued for determining appropriate safeguards.
    4. Whether to add standards to prevent CoC and CP access to covered data.
5. How to further define privacy-enhancing technologies that could be used to mitigate restricted transactions.
6. Whether the quantitative standards for data aggregation in the CISA requirements should track the bulk-data thresholds in the NPRM.
7. The potential for CoCs or CPs to defeat the security measures CISA proposed using current or anticipated future technology.
8. Whether there would be a benefit to mapping the CISA security requirements to existing standards, such as ISO-27001 or NIST Special Publication 800-171.

Conclusion

U.S. businesses that engage in restricted transactions should work with security and legal professionals to ensure compliance with the rules DOJ and CISA have announced and to track relevant developments as DOJ and CISA respond to public comments.

Authors

Explore more in

Privacy & Security Data Security Counseling and Breach Response Life Sciences & Healthcare Technology & Communications

Related insights

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law

Update

February Tip of the Month: Federal Court Issues Nationwide Injunction Against Trump Executive Orders on DEI Initiatives