DEPARTMENT OF HOMELAND SECURITY

[Docket No. CISA-2024-0029]

Notice of Availability of Security Requirements for Restricted Transactions Under Executive Order 14117

AGENCY: Cybersecurity and Infrastructure Security Agency (CISA), DHS.

ACTION: Notice of availability

SUMMARY: CISA is announcing publication of finalized security requirements for restricted transactions pursuant to Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern." In October 2024, CISA published proposed security requirements for restricted transactions which would apply to classes of restricted transactions identified in regulations issued by the Department of Justice (DOJ). CISA solicited comment on those proposed security requirements and considered that public feedback when developing the final security requirements. This notice also provides CISA's responses to the public comments received.

DATES: [INSERT DATE OF PUBLICATION IN THE *FEDERAL REGISTER*].

ADDRESSES: *Docket*: For access to the docket to read background documents or comments received, go to www.regulations.gov, and insert the docket number, CISA-2024-0029, into the "Search" box, and follow the prompts.

FOR FURTHER INFORMATION CONTACT: Alicia Smith, Senior Policy Counsel, Cybersecurity and Infrastructure Security Agency, EOSecurityReqs@cisa.dhs.gov**,** 202-316-1560.

SUPPLEMENTARY INFORMATION:

I. Background

On February 28, 2024, the President issued E.O. 14117 entitled "Preventing Access to Americans' Bulk Sensitive Personal Data and U.S. Government-Related Data by Countries of Concern" (the "Order"), pursuant to his authority under the Constitution and laws of the United States, including the International Emergency Economic Powers Act (50 U.S.C. 1701 *et seq.*) ("IEEPA"), the National Emergencies Act (50 U.S.C. 1601 *et seq.*), and section 301 of Title 3, United States Code. In the Order, the President expanded the scope of the national emergency declared in E.O. 13873 of May 15, 2019, "Securing the Information and Communications Technology and Services Supply Chain," and further addressed the national emergency with additional measures in E.O. 14034 of June 9, 2021, "Protecting Americans' Sensitive Data from Foreign Adversaries." Specifically, Section 2(a) of E.O. 14117 directs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, to issue, subject to public notice and comment, regulations that prohibit or otherwise restrict United States persons from engaging in any acquisition, holding, use, transfer, transportation, or exportation of, or dealing in, any property in which a foreign country or national thereof has any interest ("transaction"), where the transaction: (i) involves bulk sensitive personal data or United States Government-related data, as defined by final rules implementing the Order; (ii) is a member of a class of transactions that has been determined by the Attorney General to pose an unacceptable risk to the national security of the United States because the transactions may enable countries of concern or covered persons to access bulk sensitive personal data or United States Government-related data in a manner that contributes to the national emergency described in the Order; and (iii) meets other criteria specified by the Order.[1]

[1] The other criteria do not directly impact the development of the security requirements but are related to DOJ's implementation of the Order's directive via their regulations. *See* E.O. 14117, sec. 2(a)(iii)—(v), 89 FR 15421, 15423 (Mar. 1, 2024).

Among other things, the Order, at Section 2(c), instructs the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, to issue regulations identifying specific categories of transactions ("restricted transactions") that meet the criteria described in (ii) above for which the Attorney General determines that security requirements, to be established by the Secretary of Homeland Security through the Director of CISA, adequately mitigate the risks of access by countries of concern or covered persons[2] to bulk sensitive personal data or United States Government-related data. In turn, Section 2(d) directs the Secretary of Homeland Security, acting through the Director of CISA, to propose, seek public comment on, and publish those security requirements. Section 2(e) delegates to the Secretary of Homeland Security the President's powers under IEEPA as necessary to carry out Section 2(d).

On October 29, 2024, CISA published a *Federal Register* notice, Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117 (the "October 29 Request for Comment"), announcing the release of the "Proposed Security Requirements for Restricted Transactions"[3] directed by E.O. 14117 Section 2(d) and requesting public comment on the proposal. *See* 89 FR 85976. The proposed security requirements were developed to apply to the classes of restricted transactions identified in DOJ's notice of proposed rulemaking (NPRM), "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons," and published in the *Federal Register* on the same day as the proposed security requirements. *See* 89 FR 86116.

---

[2] Section 2(c)(iii) of the Order requires the Attorney General to identify, with the concurrence of the Secretaries of State and Commerce, countries of concern and, as appropriate, classes of covered persons for the purposes of the Order.

[3] The proposed security requirements were posted at https://www.cisa.gov/resources-tools/resources/proposed-security-requirements-restricted-transactions.

The DOJ NPRM proposed to require, consistent with E.O. 14117, that United States persons engaging in restricted transactions must comply with the final security requirements by incorporating the standards by reference. *See* proposed 28 CFR 202.248, 202.401, 202.402.

The security requirements were divided into two sections: organizational- and covered system-level requirements (Section I) and data-level requirements (Section II). The listed requirements were selected with the intent of directly mitigating the risk of access to covered data, with additional requirements included to ensure effective governance of that access, as well as approaches for establishing an auditable basis for compliance purposes. The security requirements further included a definitions section. To the extent the requirements used a term already proposed to be defined in the DOJ rulemaking, CISA's use of that term in the security requirements would carry the same meaning. The October 29 Request for Comment described the proposed security requirements and definitions, and further provided a non-exhaustive list of twelve questions to assist members of the public in formulating their comments.

CISA received 24 comments on the proposed security requirements and considered them while developing the final security requirements. Comments submitted in response to the October 29 Request for Comment are available in the docket associated with this notice available at *https://www.regulations.gov* (Docket CISA-2024-0029). DOJ's NPRM received 75 comments, which are available in the docket associated with that NPRM at *https://www.regulations.gov* (Docket DOJ-NSD-2024-0004-0001). DOJ shared comments with CISA that DOJ received in response to the NPRM that provided feedback that could impact the security requirements. These comments include one confidential comment that contained CISA equities and was provided to DOJ by a foreign government.

II. Response to Public Comments

A. In General

CISA reviewed and considered all comments received in response to the October 29 Request for Comment. Overall, many commenters appreciated the flexibility that CISA provided regarding implementation of the security requirements as well as the use of existing frameworks. Some commenters, however, felt that application of the security requirements as proposed may be burdensome. Others requested clarification of certain definitional terms and the scope of the security requirements. Some commenters also provided specific feedback on technical elements of the proposed security requirements. CISA addresses those comments in the following sections and explains where CISA made changes to its proposal to address the feedback received.[4]

B. Specific Topics

1. Responses to Questions in CISA's Notice

In the October 29 Request for Comment, CISA included a non-exhaustive list of twelve questions to assist the public in providing comments in response to the notice. *See* 89 FR 85980. The comments CISA received on those questions, and CISA's adjudication of those comments, are summarized below.

Robustness, Burden, and Flexibility of Proposed Security Requirements

In the October 29 Request for Comment, CISA solicited comments on whether the proposed security requirements were sufficiently robust to mitigate the risks of access to Americans' bulk sensitive personal data or government-related data by countries of concern (question 1). CISA also asked whether the security requirements provided sufficient flexibility for the types of restricted transactions typically engaged in by U.S.

[4] CISA also participated in several stakeholder engagement sessions organized by DOJ. While CISA did not receive written feedback during these sessions, many points raised by stakeholders in these sessions were echoed in the written comments received in response to the October 29 Request for Comment.

entities to avoid overburdening commercial activities not involving covered data (question 3).[5]

Many commenters either suggested or explicitly stated that the security requirements were sufficiently robust to mitigate the risk of access to covered data by countries of concern, but may be too prescriptive or burdensome to implement.[6] For instance, while commenters generally appreciated CISA's use of established frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF), a small number of commenters questioned whether CISA's security requirements extend beyond those frameworks and suggest more prescriptive mandates that may be difficult to implement.[7] Other commenters acknowledged that organizations that will be required to comply with this rule already employ some level of sophisticated cyber defense measures, but it will take time for organizations to understand, interpret, and fully implement the requirements,[8] particularly for small- and medium-sized businesses.[9] One financial sector association noted that, for financial institutions with large, diverse networks, implementation would be resource-intensive and may not be feasible in some circumstances.[10]

Several commenters expressed appreciation for the flexibility embedded in the data-level requirements in Section II, noting that flexibility encourages a risk-based but tailored approach to securing transactions, and would help ensure the requirements stay up-to-date as standards are updated and technology advances.[11] For that reason, many

---

[5] Other aspects of question 3 related to the clarity and specificity of the security requirements are addressed separately below.
[6] *See, e.g.*, Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by ACT|The App Association, CISA-2024-0029-0001.
[7] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.
[8] *See, e.g.,* Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.
[9] *See, e.g.*, Comment submitted by Consumer Technology Association, CISA-2024-0029-0013.
[10] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.
[11] *See, e.g.*, Comment submitted by Workday, CISA-2024-0029-0019.

commenters encouraged CISA to extend such flexibility to the organizational- and system-level requirements in Section I.[12]

Some commenters suggested that organizations be permitted to employ alternative compensating controls on covered systems where requirements are otherwise infeasible.[13] Others urged CISA to model the security requirements on existing regulatory regimes administered by other U.S. government agencies (*e.g.,* the Federal Communications Commission and the Department of Commerce), which direct organizations to develop cyber risk management plans aligned with the CSF, or create avenues for reciprocity in instances where U.S. entities entering into restricted transactions are subject to and have demonstrated compliance with certain existing data or cybersecurity regulatory regimes.[14] Commenters suggested that not providing the requested flexibility, modeling, or reciprocity would increase the burden on parties engaged in restricted transactions.[15]

CISA considered these options but ultimately concluded that the overall structure and approach of the original security requirements provide as much flexibility as reasonably practicable while still addressing the national security risks identified by DOJ. CISA assesses that granting reciprocity where U.S. entities entering into restricted transactions are subject to and have demonstrated compliance with certain existing data or cybersecurity regulatory regimes is not a workable solution to address the national security risks associated with restricted transactions. Other regulatory regimes are not

---

[12] *See, e.g.*, Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017; Comment submitted by Workday, CISA-2024-0029-0019; Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by ACT|The App Association, CISA-2024-0029-0001.

[13] *See, e.g.*, Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015.

[14] *See, e.g.*, Comment submitted by CTIA – The Wireless Association and NCTA – The Internet & Television Association, CISA-2024-0029-0021; Comment submitted by USTelecom – The Broadband Association, CISA-2024-0029-0018.

[15] *See, e.g.*, Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017; Comment submitted by Workday, CISA-2024-0029-0019; Comment submitted by Oracle, CISA-2024-0029-0014.

necessarily designed to address the specific risks at issue here. Therefore, CISA cannot assume that a cyber risk management plan developed to comply with another regulatory regime will necessarily be designed in a way that mitigates the risk of covered persons or countries of concern gaining access to covered data. Further, even if CISA were to do a comparison to map the security requirements against the requirements in other regulatory regimes and identify existing regulatory regimes that cover all of the security requirements today, CISA could not control for the possibility that those regulations may be changed to no longer align with the security requirements, particularly in light of the different goals of these regulations.

That said, CISA is taking a number of steps to make the final security requirements less burdensome and address specific concerns about technical feasibility or ease of implementation with respect to individual requirements. Specifically in the following sections of the security requirements:

- I.A.1.a: CISA acknowledges the challenge of maintaining an accurate asset inventory in dynamic environments, and revises I.A.1.a to require documented inventories only "to the maximum extent practicable," and eliminated the requirement to inventory MAC addresses, which is not possible in some situations such as cloud environments. CISA also clarified that these inventories can themselves be dynamically curated.
- I.A.3: CISA addresses commenters' concerns about the rigidity, utility, and feasibility of the proposed vulnerability remediation timelines, and substantially revises the vulnerability remediation timelines to prioritize critical assets and allow entities engaged in restricted transactions to remediate vulnerabilities within a risk-informed span of time. CISA assesses that these new requirements appropriately balance the risks of exploitation of vulnerable covered systems with the operational burden of patching systems.

- I.A.5: In response to comments about the level of effort required to implement the security requirements across large enterprises,[16] CISA revises the requirement for any network interfacing with a covered system to facilitate visibility into connections between assets to be implemented "to the extent technically feasible" instead of "to the maximum extent practicable."
- I.A.6: To grant organizations additional flexibility in how they choose to perform change management, CISA significantly reduces the burden around installation of new hardware and/or software by removing the reference to "firmware" and requirements for either allowlists or approvals to address specific software versions.[17]
- I.B.2: CISA seeks to introduce flexibility and alleviate confusion around the meaning of the term "immediately" by revising the requirement to revoke access to covered systems for terminated employees or employees with changed roles from "immediately" to "promptly," with clarifying examples of what would be considered "promptly." CISA recognizes the ambiguity of "immediately" and assesses that the clarifying examples appropriately balance operational complexity and the security benefits of promptly revoking access to covered data upon termination or change of an employee's role.
- I.B.3: Acknowledging the term "disabled" is ambiguous and that commenters requested CISA clarify that the requirement was to implement a process, CISA clarifies language around security log retention to state that organizations are required to implement a notification process when security logs are not being produced and/or retained as expected rather than referring to logs being disabled.

[16] *See, e.g.*, Comment submitted by U.S. Chamber of Commerce, CISA 2024-0029-0017.
[17] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

- I.B.4 [removed]: To reduce burden on implementing organizations, CISA removes the requirement to maintain organizational policies and processes to ensure that unauthorized media and hardware are not connected to covered assets. CISA assesses that in light of CISA's updates to the definition of the term "covered system," the other requirements are sufficient to protect covered systems, and this requirement is no longer necessary. [Note that, as a result of this deletion, requirements I.B.5 and 6 are now I.B.4 and 5.]
- I.B.5 [renumbered I.B.4] CISA clarifies that deploying "deny by default" is not as burdensome as some commenters assumed by noting the idea of "deny by default" does not only include the use of network firewalls but may also be implemented in other ways, such as via authentication of users and other information systems to the covered system. CISA assesses that, as clarified, this requirement is important to ensure that unauthorized systems and users do not inappropriately have access to data within covered systems.

At the same time, when crafting the proposed security requirements, CISA did so with the goal of balancing regulatory burden, technical feasibility, and flexibility with the underlying national security needs. As such, CISA determined that certain recommendations, such as extending the flexible implementation approach in the data-level requirements to the organizational- and system-level requirements, would undermine security to the detriment of the overall regime. CISA notes that the organizational- and system-level requirements are scoped only to a limited subset of covered systems that interact with data of particular sensitivity (per the DOJ rule) and are neither considered nor intended to comprise the entirety of an effective cybersecurity program; rather, they are a selected set of practices and preconditions that CISA concluded are necessary to effectively implement the data-level requirements.

Clarifying Terms and Applications

CISA asked whether the security requirements were sufficiently clear for organizations to verify compliance (question 3) and/or sufficient to provide U.S. persons engaged in restricted transactions confidence that the logical and physical access controls are sufficiently managed to deny access to covered persons or countries of concern (question 2). CISA also asked about areas where additional interpretive guidance would be helpful to U.S. entities in determining which data-level requirements should be applied based on the nature of the transaction and the data at hand (question 6).

Some commenters requested that CISA clarify the definition of "covered system," specifically as it relates to endpoints (*e.g.,* workstations/laptops), to make clear that the definition only applies to systems that handle covered data qualified as bulk under DOJ's definition.[18] One commenter observed that "this interpretation is of critical importance as it represents the difference between organizations considering how they secure a collection of specific systems as opposed to an enterprise-wide retooling, the latter of which would be extremely challenging and unnecessarily burdensome."[19]

In response, CISA revises the definition of "covered system" to reflect that a covered system is limited to systems that interact with covered data in bulk form and not user endpoints that ordinarily read or view sensitive personal data (other than sensitive personal data that constitutes government-related data) but do not ordinarily interact with sensitive personal data in bulk form. Of note, because government-related data is not subject to any bulk data threshold in the DOJ rulemaking, any system that interacts with government-related data would still be considered a covered system. Organizations implementing the security requirements need to carefully consider how this clarification applies to their particular information systems, transactions, and manners of interacting with covered data.

---

[18] *See, e.g.*, Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.
[19] Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.

CISA also received comments requesting that, in defining "covered systems" and "covered data," CISA include an explicit reference to exempt transactions by specifically exempting data that is subject to an exemption from the definition of covered systems and covered data.[20]

CISA notes that both definitions in the security requirements require the system and/or data to be used "as part of a restricted transaction." Per the definitions in the DOJ rulemaking, an exempt transaction is definitionally not a restricted transaction and thus an information system that *exclusively* participates in transactions with covered persons that are exempt (*e.g.*, an internal human resources system that only deals in data subject to the corporate group exemption) would not be considered a covered system under the definition. Because CISA assesses that the definition already excludes such systems, CISA does not make any changes to the definition in response to these comments. However, consistent with changes to the DOJ rulemaking to switch the order of the terms "government-related data" and "bulk U.S. sensitive personal data" to avoid the possibility of confusion as to whether the bulk thresholds apply to government-related data, CISA has revised the definition of "covered data" to switch the order of these terms in the definition.

Mapping to Other Frameworks

In the October 29 Request for Comment, CISA inquired about the utility of mapping requirements to other standards, such as ISO/IEC 27001 or NIST Special Publication 800-171 (question 12). Some commenters recommended this approach, noting that such mapping would be helpful to allow organizations to better understand how existing processes or controls they are already using can be applied and understood

[20] *See, e.g.*, Comment submitted by WorkDay, CISA-2024-0029-0019.

in the context of the security requirements.[21] Other commenters suggested additional candidates (*e.g.,* CISA's Encrypted DNS Implementation Guidance).[22]

CISA determined additional mapping is better suited to interpretive guidance because these frameworks include detailed security control sets, and such guidance will need to further clarify the intent and extent of the mapping to these controls. CISA decided not to include additional mapping in the final security requirements themselves but remains open to providing additional mapping through future interpretive guidance.

2. Other Comments on the Security Requirements

Extent to Which Covered Persons May Access Covered Data

Several commenters inquired if CISA's security requirements were intended to prevent all access to covered data by covered persons or to prevent unauthorized or unmitigated access.[23] That is, commenters sought clarity on whether any degree of access by covered persons to covered data is permissible when implementing the security requirements. Commenters noted, for instance, that the chapeau of Section II of the security requirements indicated that entities were required to prevent covered persons or countries of concern from gaining access to covered data, which would appear to render the transaction no longer covered by DOJ's rule.[24] Commenters explained that under their reading, the requirement to prevent access to covered data by covered persons or countries of concern arguably takes the transaction out of the DOJ rule's definition of restricted transaction altogether.[25] Commenters noted, however, that CISA's security requirements were developed to suggest the efficacy of controls such as data

---

[21] S*ee, e.g.*, Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015; Comment submitted by ACT|The App Association, CISA-2024-0029-0023.
[22] S*ee, e.g.*, Comment submitted by Infoblox, CISA-2024-0029-0020.
[23] *See, e.g.*, Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017; Comment submitted by the Consumer Technology Association, CISA-2024-0029-0013; Comment submitted by National Foreign Trade Council, CISA-2024-0029-0022.
[24] *See, e.g.*, Comment submitted by U.S. Chamber of Commerce, CISA-2024-0029-0017.
[25] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

minimization, masking, and privacy-enhancing techniques in mitigating the risk of access to covered data by covered persons or countries of concerns.

To address the feedback raised in these comments, CISA affirms that the security requirements are meant to prevent access to covered data by countries of concern unless specific efforts outlined in the security requirements are taken to mitigate the national security risks associated with such access.

More specifically, in the chapeau to the data-level requirements in Section II, CISA proposed that U.S. persons should "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." CISA proposed that this approach would mitigate the national security risks associated with access to covered data by covered persons and/or countries of concern. As described in the Order, DOJ's NPRM, and CISA's proposed security requirements and the October 29 Request for Comment, access to covered data by covered persons and/or countries of concern poses a range of threats to national security and foreign policy, including providing countries of concern with information they need or can use to engage in malicious cyber-enabled activities and malign foreign influence; blackmail and espionage against U.S. persons; intimidate activists, academics, journalists, dissidents, political figures, or members of non-governmental organizations or marginalized communities; curb political opposition; limit freedoms of expression, peaceful assembly, or association; or enable other forms of suppression of civil liberties. *See* 89 FR 85978. In the security requirements, CISA proposed to address these risks at the data level by requiring that covered persons be denied access to the underlying covered data – either by denying access outright or by only allowing covered persons access to covered data that had been manipulated in a way (*e.g.*, encryption, de-identification) that would effectively mitigate the risks from permitting direct access to the underlying data.

In response to comments on this issue, CISA clarifies the chapeau language for the data-level requirements in the final security requirements to state that U.S. persons should "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." This clarification establishes that the adoption of the data-level requirements does not mean no access to covered data is permissible, but that certain data-level requirements must be implemented to achieve a level of minimization of that access and/or covered data sufficient to mitigate the national security risks identified by DOJ.

Under the DOJ regulation, covered data transactions include regulated categories of transactions that involve covered person or country of concern access to covered data, regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified. As DOJ explains in its rulemaking, encryption, pseudonymization, and de-identification are not completely effective in all cases and can in some cases be reversed or undermined. At the same time, the transactions identified by DOJ as restricted have important economic value relative to their national security risk and are allowed to proceed if they meet the CISA-developed security requirements. CISA was thus tasked with determining an appropriate balance on mitigating the national security risks associated with such access to covered data.

While CISA considered whether it could adopt other options for data-level requirements that would still permit access to at least some unmitigated covered data to covered persons, CISA ultimately determined that allowing covered persons or countries of concern access to covered data without application of an effective combination of techniques identified in the data-level requirements (such as pseudonymization, de-identification, aggregation, and encryption) would not effectively mitigate the

unacceptable national security risks identified by DOJ resulting from enabling access to such data by covered persons and countries of concern. Thus, the final security requirements permit organizations to undertake restricted transactions either by directly denying covered person/country of concern access to covered data itself or by applying techniques such as pseudonymization, de-identification, aggregation, and encryption in the manner prescribed in the security requirements to reduce the risks to national security while still allowing for a form of access to an appropriately mitigated version of the covered data (in conjunction with implementation of the organizational- and system-level requirements).

As noted in the DOJ regulation's definition of access, the implementation of data processing techniques (as outlined in the data-level requirements) before sharing data is irrelevant to the determination of whether a transaction involves "access" and is thus a covered data transaction. However, restricted transactions are explicitly permitted to proceed through application of the security requirements, effectively mitigating the national security risks identified by DOJ.

The following examples discuss several applicable scenarios. In all cases (with the exception of example 4), these examples assume that the organization has conducted the required data risk assessment required in Section I.C of the security requirements and determined that the specific requirements implemented are 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." The examples (with the exception of example 4) also assume that the organization complies with other applicable requirements in the DOJ's rule.

Example 1: A U.S. person retains a cloud provider headquartered in a country of concern to store encrypted covered data through a vendor agreement. Per the DOJ rulemaking, the cloud provider is a covered person, and such a transaction would

constitute a covered data transaction. The U.S. person implements the security requirements, including the requirements around encryption and encryption keys. Such a transaction could proceed if the U.S. person fully implements the security requirements.

Example 2: A U.S. business that deals in covered data is executing an investment agreement with a covered person. The investment agreement provides that the U.S. business will share with the covered person investor sensitive personal data about individual consumers that meets DOJ's relevant bulk threshold. The organization implements the security requirements before sharing data with the covered person investor (for example by aggregating data and/or de-identifying it along with implementing the other security requirements). Such data is still considered covered data. The sharing of data in the investment agreement is still a restricted transaction but can proceed due to the implementation of the security requirements.

Example 3: A U.S. organization hires a covered person in a country of concern (or retains their services by contract) into a role whose duties include access to covered data. As part of entering into the employment agreement (or vendor agreement), the organization implements the security requirements (including the organizational- and system-level requirements) and only shares de-identified covered data with the covered person in a way that minimizes linkability in accordance with the security requirements. Such a restricted transaction would be allowed to proceed.

Example 4: Same as Example 3, except that instead of de-identifying the covered data, the organization knowingly authorizes the employee or vendor to have access to covered data (*e.g.*, to bulk U.S. sensitive personal data) without applying efforts to de-identify, pseudonymize, encrypt, or otherwise implement the data-level security requirements. In this example, the U.S. organization knowingly gave a covered person access to covered data through an employment or vendor agreement without implementing the security requirements. As such, the U.S. organization knowingly

engaged in a restricted transaction that fails to comply with the requirements of subpart D of 28 CFR part 202 and thus is engaged in a covered data transaction that is not authorized pursuant to 28 CFR 202.401.

Example 5: Same as Example 3, except the employee or vendor's duties do not require access to covered data but do include general access to the organization's networks and information systems, including potentially covered systems, within which covered data may be stored. The organization implements the security requirements, including the data-level requirement of denying access to covered data for that covered person. Because the transaction could afford a covered person access to covered data, but the organization employed controls to prevent it, such an employment or vendor agreement could proceed as a restricted transaction.

Vulnerability Management (I.A.3)

In the proposed security requirements, CISA proposed that organizations should patch vulnerabilities that are known to be exploited, critical, or high within an outlined timeframe. CISA proposed this approach for consistency with the standard to which Federal Agencies are held under Binding Operational Directives (BOD) 22-01 and 19-02. CISA received several comments on this subject suggesting that CISA's approach was technically challenging to implement and not sufficiently risk-based.[26] One commenter, for instance, stated that the remediation timelines proposed were too aggressive, and noted that NIST Special Publication 800-53 directs remediation to occur in accordance with a risk-assessment rather than prescribing specific timelines.[27] Another commenter recommended that CISA change the timelines for remediation to no shorter than 30 days, stating that CISA's proposed timeframes of 14 and 15 days were unreasonable and

[26] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011; Comment submitted by Consumer Technology Association, CISA-2024-0029-0013; Comment submitted by USTelecom, CISA-2024-0029-0018; Comment submitted by Information Technology Industry Council, CISA-2024-0029-0015.

[27] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011

impracticable.[28] Commenters indicated that this requirement may cause organizations to expend their limited resources addressing vulnerabilities that do not necessarily pose the greatest risk to their organizations.[29]

CISA considered this feedback carefully and concluded that an alternate approach to vulnerability management could effectively respond to the identified risks while being less burdensome in implementation. In the final security requirements, CISA adopts a new approach that requires organizations to remediate known exploited vulnerabilities (KEVs) in internet-facing systems in a risk-based manner that prioritizes the most critical assets first, with all such vulnerabilities remediated within 45 calendar days. This approach is based on the approach to patching outlined in the CISA Cross-Sector Cybersecurity Performance Goals (CPGs) and the CSF. To compensate for the additional flexibility being provided through the revised requirement, CISA determined that it was necessary to require that entities engaged in restricted transactions establish a process to evaluate, after patching, whether any internet-facing covered systems with KEVs were compromised prior to the patch being applied. Based on its operational experience, CISA notes that KEVs on internet-facing systems are commonly exploited with access persisting beyond the time of patching. A KEV is a vulnerability that is currently being exploited, based on information known to CISA.[30] Through this change, CISA intends to reduce the operational burden of vulnerability management and maximize its impact on addressing known cybersecurity risks to covered systems.

Multi-factor Authentication and Password Length (I.B.1)

In the proposed security requirements, CISA proposed that organizations should implement multi-factor authentication (MFA) for access to covered systems or, if not

---

[28] *See, e.g.*, Comment submitted by Consumer Technology Association, CISA-2024-0029-0013
[29] *See, e.g.*, Comment submitted by the Bank Policy Institute, CISA-2024-0029-0011.
[30] *See generally* Cybersecurity and Infrastructure Security Agency, Reducing the Significant Risk of Known Exploited Vulnerabilities, https://www.cisa.gov/known-exploited-vulnerabilities (last visited Dec. 1, 2024) (listing CISA's requirements for listing a KEV).

technically feasible and/or enforced, implement passwords of a minimum of 16 characters. CISA proposed this approach based on the CSF and the CISA CPGs. Commenters suggested that CISA's approach would be clearer if CISA incorporated NIST Special Publication 800-63B (SP 800-63B)'s definition of Authentication Assurance Levels (AALs) and only required 16-character passwords if technically feasible.[31]

In the final security requirements, CISA added a reference to NIST's AAL definition to clarify that CISA considers any authenticator that implements AAL2 or AAL3 (as defined in the latest version of SP 800-63B or any of its supplements) as qualifying as MFA for purposes of this requirement. This includes syncable cryptographic authenticators (colloquially known as "passkeys"). However, CISA notes that "Multi-factor authentication" is a broadly understood term in the industry and declines to remove its use from the security requirements. CISA also updates the requirement for 16-character passwords to instead require 15-character passwords in situations without MFA. This change reduces burden on organizations and aligns CISA's requirement with the CPGs. However, CISA declines to further reduce the number of required characters, even where 15-character passwords are not technically feasible. This requirement is taken from the CISA CPGs where sufficiently strong passwords are suggested for all password-protected IT assets, with an understanding that some operational technology (OT) assets may not be able to technically support such passwords. CISA does not believe such OT assets are likely to host covered data and did not receive any comments suggesting otherwise. CISA concludes that information systems that host covered data be required to either implement MFA (including "passwordless" methods) or have 15-character minimum passwords in instances where

[31] *See, e.g.,* Comment submitted by Workday, CISA-2024-0029-0019; Comment submitted by USTelecom – The Broadband Association, CISA-2024-0029-0018.

MFA is not technically feasible and/or enforced (such as when MFA is partially enforced due to technical limitations). CISA believes that organizations should implement MFA in all situations where it is technically feasible to do so and where it is not, must ensure 15-character passwords are used in covered systems. CISA assesses that this approach is a reasonable requirement that is well grounded in industry best practices. Technologies such as password managers may be used to reduce the operational burden of such passwords.

Access to Log Systems (I.B.3)

One commenter[32] requested that CISA clarify whether authorized access to the security logging system is intended to be limited to those users who are authorized to access the covered system itself or, more generally, users performing security duties in the organization.

CISA declines to make any changes to the text of the final security requirements in response to this comment, but notes that the security requirements specify that users who access or modify such log data are only required to be "authorized and authenticated." CISA does not intend that individuals who are "authorized and authenticated" to access or modify collected logs must also be authorized to access covered systems.

Data Risk Assessment (I.C)

Several commenters raised questions and concerns about the data risk assessment. Some commentors were concerned about whether the risk assessment was to be shared with DOJ or CISA, while others had some concerns about the potential cost impact and compliance burden of developing it. Others also noted that DOJ included audit and

[32] *See* Comment submitted by The Business Software Alliance, CISA-2024-0029-0024.

reporting requirements in its rule and that the addition of another compliance report under CISA's requirements would be too burdensome.[33]

In response to these comments, and to deconflict with DOJ's audit and reporting requirements, CISA makes minor changes to this requirement, specifically clarifying this risk assessment is intended for internal use only as a tool to inform data protection (not for documentation or disclosure to a government agency), and, to further reduce implementation burden, that documenting the assessment is not required.[34] CISA also supplies additional detail specifying that the plan be reviewed internally by the organization.

Data-Level Requirements and What Constitutes "Sufficiency" (II, Chapeau)

Comments pertaining to the data-level requirements were largely positive, noting an appreciation for the level of flexibility that was perceived by many to be in contrast with the system-level requirements. For instance, one commenter said that allowing organizations flexibility to determine which combination of data-level requirements are sufficient to address risks, based on their unique risk profile "presents the best chance of achieving Executive Order 14117's ultimate objective to secure" sensitive U.S. data.[35] However, some commenters took issue with the requirement to *fully* and effectively prevent access to covered data, and requested guidance and/or clarification about what constitutes a "sufficient" combination of data-level requirements to prevent access. CISA also received some feedback from interagency partners on further clarifying the specific encryption requirements.

Given that commenters generally agreed that the data-level requirements as written achieved their intended aim, CISA made only minor revisions. Commenters

---

[33] *See, e.g.*, Comment submitted by The Consumer Technology Association, CISA-2024-0029-0013.
[34] CISA defers to DOJ regarding whether such a risk assessment may be subject to audit or other review as part of compliance aspects of the DOJ rulemaking.
[35] *See, e.g.*, Comment submitted by Bank Policy Institute, CISA-2024-0029-0011.

asked CISA to clarify that requirements around the version of Transport Layer Security (TLS) used were limited to connections that were already using TLS, which CISA clarified by including requirements for the version of TLS in II.B.1 rather than as a separate requirement (II.B.2). CISA also consulted with other federal agency partners on the topic of encryption and is adding an explanation of what level of encryption CISA considers sufficient for the purposes of these security requirements based on these consultations. CISA recognizes the appeal of a prescriptive (and predictable) standard but maintains there is no one-size-fits-all solution given the varied nature of restricted transactions. Additionally, the question of what is sufficient to prevent access is a compliance matter and not a technical implementation matter. E.O. 14117 sec. 2(d)(ii) gives the Attorney General authority to issue enforcement guidance regarding these security requirements, in consultation with the Director of CISA. CISA will coordinate with DOJ if it determines further guidance on the meaning of "sufficient" is appropriate.

Framework Mapping

Many commenters expressed appreciation for the fact that CISA leveraged existing, well-known cybersecurity and privacy frameworks, and found the mapping between frameworks and specific requirements especially helpful. However, some commenters expressed concern that CISA's approach was not conducive to harmonizing cyber regulations to the greatest degree practicable across the government and suggested that CISA's mapping to the CSF, NIST's Privacy Framework (PF), and CPGs may be confusing, noting that the CSF is the primary risk management framework used by some organizations.

After considering these comments, CISA continues to assess that its method of mapping the security requirements to the CSF, PF, and CPGs is the optimal way to minimize the burden on organizations while still allowing as much flexibility in implementation as possible.

First, as noted in the proposed security requirements and as CISA has preserved in the final security requirements, references to these frameworks are intended to help readers understand which aspects of existing frameworks, guidance, or other resources the security requirements are based upon; understanding and applying the security requirements *does not* require a reader to understand and apply those references. As such, the references should only serve to be a helpful reference where readers find them useful, while those who find the references confusing or who do not use these other resources as part of their organizational compliance structure can disregard the mapping.

Second, the Order requires CISA to base its security requirements on the CSF and the PF. CISA has evidenced compliance with this requirement by reference to these frameworks explicitly. This means that the only framework CISA could eliminate the mapping to is the CPGs. Given that many commenters expressed appreciation for the CPG mapping and that the CPGs are, themselves, based on the CSF, CISA assesses that the inclusion of the CPGs should not be overly difficult or confusing, especially for the cybersecurity personnel and designated accountable officials responsible for ensuring that U.S. entities engaging in restricted transactions adhere to the final security requirements.

3. *Out of Scope or Related to DOJ's NPRM*

Several commenters raised questions, concerns, or feedback that were outside of the authorities and direction provided to CISA in E.O. 14117. Commenters also raised issues that were related to the implementation of DOJ's regulations rather than the proposed security requirements themselves.

While CISA reviewed this feedback and shared relevant comments with DOJ to consider as they drafted their final rule, issues specific to the DOJ rule itself are beyond the scope of this notice. Conversely, in some instances, DOJ received comments on its NPRM that more directly related to CISA's proposed security requirements. Where DOJ

shared such comments with CISA, CISA reviewed and considered this feedback as part of developing the final security requirements, as reflected above.

4. Continued Stakeholder Engagement

CISA also received a few comments requesting additional stakeholder engagement on the development of these security requirements. For example, one comment requested an extension of the comment period by 17 days to provide stakeholders extra time to provide robust and considered input.

CISA appreciates the commenters' desire to provide the most useful, robust, and thoughtful feedback possible in the time allotted for comments. However, CISA decided not to extend the comment period given the pressing national security interests underlying the need for DOJ's rule, and E.O. 14117's requirement that the rule incorporate CISA's security requirements.

Other commenters requested that CISA establish an ongoing stakeholder engagement process to receive continued feedback on the security requirements even after they have been finalized. Some of the commenters noted that these security requirements could be burdensome to implement effectively, and others emphasized that experience applying the security requirements could lead stakeholders to identify areas for improvement.

CISA appreciates stakeholder interest in ensuring that the security requirements remain current and applicable over time and will consider the best way to receive and incorporate relevant feedback in the future to the extent changes to the security requirements become necessary or desirable. However, at this time, CISA does not intend to establish a formal process for receiving additional feedback on the security requirements given that the comment period has closed, and CISA must finalize the security requirements so that they can be incorporated by reference into DOJ's final rule.

One commenter expressed concern about the security requirements being a "quasi-rule," indicating that CISA could change the security requirements at any point in the future without "procedural protections" for impacted entities.[36]

CISA appreciates the concern raised by the commenter and confirms that CISA has no intention of changing these security requirements without providing the public notice of any future changes. As discussed above, CISA notes that while the Order directed DOJ to propose a rule and finalize that rule to implement its directive, the Order did not provide the same direction to CISA for promulgating the security requirements. By design, the security requirements themselves are not a rule governed by the process laid out in the Administrative Procedure Act, 5 U.S.C. 553. While this allows CISA to update the security requirements quickly, tracking new developments in technology and data security, such updated security requirements will not be enforceable against entities regulated by DOJ's rule unless DOJ updates its rule to change the version of the security requirements incorporated therein by reference. In other words, commenters can be assured that they will not be subjected to new security requirements without receiving requisite procedural protections for implementing the change, as required by law.

III. Description of Final Security Requirements

The security requirements are intended to address national-security and foreign-policy threats that arise when countries of concern[37] and covered persons access U.S. government-related data or bulk U.S. sensitive personal data that may be implicated by the categories of restricted transactions. Additional background on the purpose for these security requirements was included in CISA's notice announcing the release of the proposed security requirements. *See* 89 FR 85978. The DOJ Final Rule requires, consistent with E.O. 14117, that United States persons engaging in restricted transactions

[36] *See, e.g.*, Comment submitted by The Business Software Alliance, CISA-2024-0029-0024.
[37] Terms used in CISA's security requirements that are defined in the DOJ rulemaking have the same meaning in the security requirements as provided in the DOJ rulemaking.

comply with the final security requirements by incorporating the security requirements by reference into the regulations. 28 CFR § 202.401.

The security requirements remain divided into two sections: organizational- and covered system-level requirements (Section I) and data-level requirements (Section II). The listed requirements were selected with the intent of directly mitigating the risk of access to covered data, with additional requirements included to ensure effective governance of that access, as well as approaches for establishing an auditable basis for compliance purposes. Requirements that directly mitigate the risk of access include I.B.1-2, I.B.4-5, and all data-level requirements (II.A, II.B, II.C, and II.D). Requirements included as a mechanism for ensuring proper implementation and governance of those access controls include all controls in I.A. Additional requirements incorporated as a mechanism for ensuring auditable compliance of the aforementioned access controls include I.B.3 and I.C. These requirements reflect a minimum set of practices that CISA assesses are required for effective data protection, as informed by CISA's operational experience. These requirements were designed to be representative of broadly accepted industry best practices and are intended to address the needs of national security without imposing an unachievable burden on industry.

The final security requirements largely maintain the same design as the proposed security requirements. 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.[38] They do this by imposing

[38] CISA notes that the security requirements are, as required by the Order, 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 CPGs, available at https://www.cisa.gov/cross-sector-cybersecurity-performance-goals, are not reflected in the proposed 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.

conditions specifically on the *covered data* that may be accessed as part of a restricted transaction, on the *covered systems* more broadly (both terms CISA defines within the security requirements), 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 continues to assess 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 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 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 which 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 unmitigated covered data. The security requirements provide multiple options to mitigate risk, though all the options build upon the foundation of the requirements imposed on covered systems and the organization as a whole. While

U.S. persons[39] engaging in restricted transactions will be required to implement all the organizational- and system-level requirements, such persons will have some flexibility to determine which combination of data-level requirements are 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, based on the nature of the transaction and the data at issue.

Finally, the security requirements include a definitions section. To the extent the requirements use a term already defined in the DOJ rulemaking, CISA's use of that term in the security requirements would carry the same meaning. For the purpose of these security requirements, CISA includes definitions for five terms used exclusively in the security requirements:

- *Asset*. CISA defines the term to mean data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes. This definition is derived from the CSF version 1.1, which defined asset as "[t]he data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes."
- *Covered data*. CISA defines the term to mean the two categories of data identified by the Order and that DOJ is regulating through its rulemaking –government-related data or bulk U.S. sensitive personal data.
- *Covered system.* CISA defines this term as a specific type of information system that is used to conduct a number of activities related to covered data as part of a restricted transaction. These activities are drawn from a combination of the activities in the definition of information system in the security requirements and the activities in the

[39] As noted above, for the purposes of the security requirements, to the extent CISA uses a term that is defined in the DOJ rulemaking, CISA uses that definition. Therefore, CISA is using the term U.S. persons as defined by the DOJ Final Rule. That definition reads "any United States citizen, national, or lawful permanent resident; any individual admitted to the United States as a refugee under 8 U.S.C. 1157 or granted asylum under 8 U.S.C. 1158; any entity organized solely under the laws of the United States or any jurisdiction within the United States (including foreign branches); or any person in the United States." 28 CFR 202.256.

DOJ rulemaking's definition of access. See 28 CFR 202.201. The term 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. "Covered system" 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.

- *Information system*. CISA defines this term consistent with the definition in the Paperwork Reduction Act (PRA), 44 U.S.C. 3502.[40] The term means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
- *Network*. CISA defines this term, which CISA developed consistent with the definition of the term in NIST Special Publication 800-171 rev. 3, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations.* The term would mean a system of interconnected components, which may include routers, hubs, cabling, telecommunications controllers, key distribution centers, and technical control devices.

[40] 6 U.S.C. 650(14) (which applies to all of Title XXII of the Homeland Security Act of 2002, which, in turn, contains most of CISA's authorities) defines Information System as having the meaning given the term in the Paperwork Reduction Act, 44 U.S.C. 3502, and specifically includes "industrial control systems, such as supervisory control and data acquisition systems, distributed control systems, and programmable logic controllers." 6 U.S.C. 650(14). However, given CISA's assumption that this type of operational technology is unlikely to be implicated by DOJ's regulations, CISA is not including the operational technology-related prong here.

The publication of the finalized security requirements for restricted transactions pursuant to Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern" can be found on CISA's website: https://www.cisa.gov/resources-tools/resources/EO-14117-security-requirements. The Director of CISA, Jennie M. Easterly, has delegated the authority to approve and electronically sign this document to Nitin Natarajan, who is the Deputy Director of CISA, for purposes of publication in the *Federal Register*.

_____

Nitin Natarajan,
Deputy Director,
Cybersecurity and Infrastructure Security Agency,
Department of Homeland Security.

[FR Doc. 2024-31479 Filed: 1/3/2025 8:45 am; Publication Date: 1/8/2025]