1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

November 29, 2024

The Honorable Merrick Garland
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue NW
Washington, D.C. 20530

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Administration
CISA – NGL Stop 0630
1110 N. Glebe Road
Arlington, VA 20598

Re: Provisions Regarding Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons (Dockets NSD 104 and CISA-2024-0029)

Dear Attorney General Garland and Director Easterly:

The Consumer Technology Association (CTA) appreciates the opportunity to submit written comments on the Department of Justice's (DOJ) and the Cybersecurity and Infrastructure Security Agency's (CISA) notices of proposed rulemaking (NPRMs) regarding the implementation of Executive Order 14117 and the prevention of access to U.S. sensitive personal data and government-related data by countries of concern.[1] EO 14117 is important, not only for national security, but consistent with consumer expectations and consumer technology industry reliance on designing and delivering products for use by people, whether in households, businesses, or governments. business success requires protecting sensitive data – but governing rules also must allow legitimate business consumers and others rely on to occur. This requires narrowly tailored regulatory approaches that can address discrete national security challenges while ensuring U.S. economic competitiveness.

This submission follows our comments on DOJ's advance notice of proposed rulemaking (ANPRM) on the same topic earlier this year. In those comments, CTA made suggestions not only directed to the specific provisions of the eventual proposed rule, but also related to broader principles that DOJ should pursue to advance U.S. technological leadership and address national security challenges while maintaining economic competitiveness, collaborating with

[1] Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons, 89 Fed. Reg. 86,116 (Oct. 29, 2024); Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117, 89 Fed. Reg. 85,976 (Oct. 29, 2024).

U.S. allies and partners, and preventing harmful restrictions on cross-border data flows. CTA continues to encourage DOJ, and now CISA, to consider these principles as it proceeds with this rulemaking and other regulatory and policymaking efforts.

CTA represents the more than $505 billion U.S. consumer technology industry, which supports more than 18 million U.S. jobs. Our members are some 1300 companies from every facet of the consumer technology industry, including manufacturers, distributors, developers, retailers, and integrators, with 80 percent of CTA members being start-ups or small and mid-sized companies. CTA also owns and produces CES®—the most influential technology event in the world—which showcases and serves as a forum for discussion of international policies concerning existing and new technologies, international technology trade and investment, and global opportunities and challenges facing the consumer technology industry. CES 2025 will be January 7-10, 2025, in Las Vegas. We strongly encourage DOJ and CISA leaders and staff to participate and engage with industry at this event to understand the real world impact of the proposal.

CTA's comments proceed below based on key topics and points of feedback. CTA first comments on the NPRM released by DOJ, making broader, structural comments regarding the proposed rule and its scope and then discussing feedback on specific provisions and language; in the second section, we comment on proposed security requirements published by CISA, discussing both the specific security requirements and the general scope and policy of the CISA proposed rule.

* * *

Comments Specific to DOJ's NPRM:

1. **DOJ Should Adjust the Effective Date of the Proposed Rule to Allow Time for Compliance**

The proposed rule has no effective date; nor does it suggest any delay between the rule becoming final and the beginning of enforcement. Many CTA members are already working to establish compliance programs, but industry needs sufficient time to ensure that its operations are fully compliant with any new requirements, especially on restricted transactions and data brokerage transactions with non-covered foreign persons. This is vital for small and medium-sized U.S. businesses, which make up some 80% of CTA's membership and which have smaller monetary and personnel resources to address new requirements.

In particular, identifying covered data transactions, modifying contracts, and implementing CISA security measures will be a lengthy process, especially since the exact scope of this rule and CISA's requirements will not be known until the final rule is published. CTA recommends that DOJ include a phase-in period in the final rule, giving companies at least one year before they are expected to be fully compliant.

Additionally, many of CTA's member companies have ongoing relationships with foreign entities, including some in countries of concern, which involve data-sharing or mutual access to data. While programs to ensure compliance with the rule in new transactions would be covered by the year-long phase-in period we recommend above, the compliance process for existing relationships will be more complex. CTA therefore requests a further enforcement delay of two or three years with respect to business relationships that predate the final rule's effective date.

This will allow CTA members, and companies in a variety of sectors, to enact internal measures to address data access in existing business relationships.

2. DOJ Should Reduce or Narrow Audit and Reporting Requirements

In addition to implementing compliance programs to avoid prohibited transactions and abide by security requirements in restricted transactions, consumer technology firms will also have to adhere to the rule's administrative requirements. The compliance measures themselves are onerous, but appear to be generally necessary. But the added tasks of performing an annual, independent, external audit and reporting on rejected offers for prohibited transactions within 14 days[2]—plus creating written policies on security measures and having data compliance programs annually certified by company executives[3]—adds a major challenge for our members. These requirements are arduous for large firms, but extremely so for smaller ones. CTA expects that this will not only be very costly but may also create a practical ban on "restricted" transactions due to the added cost and burden of the additional requirements associated with them for small businesses.

CTA recommends that DOJ limit the burden of these requirements to retain successful assurances of compliance without overwhelming costs. Independent, external, annual audits as an explicit legal requirement are a rarity in this regulatory sphere, and DOJ should eliminate this cumbersome burden on industry. DOJ might instead consider random spot audits, or audit requirements for companies engaged in a high volume of restricted transactions, rather than making this a blanket requirement. Alternately, companies should be allowed to conduct internal audits to ensure compliance.

DOJ should also extend the time period in which U.S. persons must report rejected offers of restricted transactions. 14 days[4] is a very short period, and implementing internal measures to ensure consistent 14-day reporting will be both difficult and expensive. Rather, we suggest a semi-annual report on all such offers. It would perform the same task with greater efficiency and ease for industry; at most, a one-month period for reporting would certainly have the same effect.

Lastly, CTA is concerned that the reporting and audit requirements contain no protection for companies' confidential information, proprietary information, or trade secrets. U.S. companies that comply with all requirements deserve to know that the information they submit pursuant to these requirements will not be publicly disclosed or used for evidentiary purposes. CTA recommends that such protections be included in the final rule so that U.S. industry can be sure that DOJ's commitment to protecting proprietary industry information from unauthorized release is as firm as its commitment to protecting U.S. sensitive data from countries of concern.

3. DOJ Should Exempt Data Transfers Incident to Online Retail Sales

Many consumer technology firms sell a variety of products and services in online marketplaces. However, as drafted, the proposed rule could essentially prevent U.S. consumers from using online purchasing for any products from countries of concern or covered persons. Because IP

---

[2] *Id.* at 86,224.

[3] *Id.* at 86,223.

[4] *Id.* at 86,225.

addresses, basic demographic information, and financial information such as credit card numbers are key data components of any online purchase, the rule's definition of "covered personal identifiers"[5] could functionally block all e-commerce with countries of concern.

More, vague definitions for terms such as "personal financial data" and "personal health data"[6] could also be read to block online purchases from countries of concern. For instance, as mentioned in the point below, the rule could be interpreted to prevent a U.S.-based online marketplace from transmitting "bulk" orders of health-related items such as face masks to a country of concern, since each order includes information "related to" an individual's health condition. Even more concerning, while a U.S.-based payment processor might be able to pass along consumer credit card information under the financial services exemption, the rule could be read to prohibit the processor from transmitting the actual orders, since they would be information about individuals' purchase histories and are not incident to *financial* services.

DOJ should ensure the ongoing viability of internet commerce by including an exemption for data shared incident to providing, maintaining, and offering products and services in online marketplaces. Whether in relation to the covered personal identifiers necessary to place an order or the fact of the purchase itself, transmissions of information that is a necessary aspect of retail transactions should be excluded from the rule's scope.

Based on the preamble of the rule, DOJ appears to have intended the financial services exemption to be a general carve-out for "the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services."[7] However, the regulatory text of the exemption creates ambiguity on this point due to the qualifier that such exempted transactions must be "ordinarily incident to and part of the provision of financial services."[8] While DOJ aims to exempt "the transfer of personal financial data or covered personal identifiers incidental to the purchase and sale of goods and services (such as the purchase, sale, or transfer of consumer products and services through online shopping or e-commerce marketplaces…"), the actual text appears to narrowly focus on financial services institutions or payment processors rather than sellers in those marketplaces.[9]

In light of the above, CTA recommends that DOJ (i) rename the financial services exemption, referring to it instead as an exemption for "financial services and consumer transactions for goods or services;" and (ii) add the following text into Section 202.505(a): … "ordinarily incident to and part of the provision of financial services or purchase and sale of goods and services." This would eliminate ambiguity and ensure that the rule does not inadvertently stifle legitimate, non-data brokerage e-commerce transactions.

4. DOJ Should Revise the Definition of "Personal Health Data" to Exclude Inferences

CTA recognizes the importance of restricting the transmission of U.S. persons' medical information to foreign adversaries, and appreciates DOJ's action to prevent the misuse of such information. However, we are concerned that the text of the proposed rule creates significant

---

[5] *Id.* at 86,206-07.

[6] See below at (4).

[7] 89 Fed. Reg. 86,116, 86,135 (2024).

[8] *Id.* at 86,217.

[9] *Id.*

uncertainty as to the scope of this term. The present definition of "personal health data"[10] includes information that "relates to" a physical or mental health condition. This is very broad language, which could be construed to cover not only medical diagnoses or drug prescriptions but also a variety of innocuous retail purchases which might in some way "relate[]" to an individual's health condition without identifying that condition. DOJ should not overly restrict commerce and access to useful goods and services without a corresponding reduction in potential harm, as it might if the final rule could be interpreted to cover, e.g., an individual's purchase of tissues at a supermarket.

CTA therefore recommends that DOJ amend the definition of "personal health data" to include information that "identifies" an individual's health condition. Data that does not identify an individual's condition poses none of the risk for which health information is included in the rule, and should not be thus constrained.

5. DOJ Should Revise the Definition of "Covered Personal Identifiers" to Exclude Low-Risk Combinations

CTA welcomes DOJ's revision of the ANPRM to more carefully define "covered personal identifiers" in the proposed rule. The exclusion from covered information of certain types of listed identifiers in combination only with identifiers of the same type is critical to avoid an overbroad scope. By removing from the definition combinations of individuals' demographic information and combinations of individuals' network-based identifiers, DOJ appropriately narrowed the rule to avoid covering information sources such as phone books or internet history.

We recommend that DOJ further tailor the scope of "covered" identifiers by additionally excluding low-risk types of listed identifier in combination with other low-risk types. As noted in Comment 3, the combination of demographic or contact information with network-based identifiers such as IP addresses is an essential element of e-commerce. But it is also a foundational element of the vast majority of internet communication and interaction. The linking of an individual's IP address with his email address or name is an ordinary function of most transactions and operations that occur online. The purpose of DOJ's rule is to prevent the sharing of sensitive personal data with countries of concern or covered persons, but it is unclear how a linked name and IP address, without more, identifies or even suggests sensitive data. DOJ should therefore also exclude combinations of demographic and network-based identifiers from the scope of the "covered personal identifier" definition.

6. DOJ Should More Clearly Define "Data Brokerage"

Consumer technology firms engage in a vast array of legitimate business practices in the United States and all over the world. Advertising is one of these practices, and it can involve the use of bulk personal sensitive data, as can a variety of other business activities our members perform. CTA recommends that DOJ narrow and clarify the scope of the term "data brokerage" in the rule to avoid unnecessarily limiting legitimate transactions and inadvertently restricting certain primarily U.S.-based activities.

In particular, CTA recommends that DOJ clarify the scope of a data brokerage "transaction" by including a requirement that consideration be exchanged for access to the data. If DOJ is

[10] *Id.* at 86,212 (2024).

determined to include interactions where the transfer of data is not the focus of the activity, it should still include a requirement of consideration at some point to ensure that internal, incidental, and necessary transfers of data are collectively excluded from the rule's scope (rather than relying solely on limited exemptions and exclusions which may not capture all of the intended exceptions).

Similarly, DOJ should consider clarifying that a transaction constitutes "data brokerage" only where the recipient obtains some kind of ownership or rights to the data, rather than a temporary, service-based, or incidental access—which, as DOJ has recognized in the proposed rule, are situations better dealt with via restricted transactions than prohibited transactions. By referring specifically to the "sale," "licensing," or "similar commercial transactions," we understand DOJ to refer to situations where the recipient receives a "transfer" of data for its own purposes. And, indeed, Example 6 contemplates a U.S. company that sells its bulk data to its parent company in a country of concern "to help [the parent company] develop artificial intelligence technology and machine learning capabilities." By specifying that a "data brokerage transaction" recipient must receive a "right, remedy, power, privilege, or interest with respect to" the data, DOJ would clarify the scope of the prohibition and avoid overbreadth.

DOJ should also eliminate the phrase "or similar commercial transactions" from the "data brokerage" definition. The vagueness of this term makes it both unhelpful and overbroad in scope, leaving U.S. companies unsure of what transactions might be "similar" enough to be completely prohibited. Alternately, DOJ could specify exactly what is meant by "similar commercial transactions" in order to narrow the category and provide clarity. DOJ should also specify more explicitly that "data brokerage" transactions must involve sensitive personal data, ideally in the definition of "data brokerage" itself.

Lastly, DOJ should clarify that neither the "data brokerage" definition nor the broader scope of the rule apply to companies that simply provide platforms for data-sharing. If a platform provider, whether U.S. person or covered person, does not determine what data is shared or review that data, they should not have to be concerned about liability for the transactions of their clients.

7. Foreign Subsidiaries Should Have the Same Protections as Foreign Branches

CTA welcomes the exemption DOJ created for intracompany transfers of bulk sensitive personal data from the United States to countries of concern.[11] This is a sensible exemption that acknowledges that such transfers likely do not pose a national security risk given the multitude of compliance obligations already imposed on U.S. businesses related to the protection of the personal data of Americans. It also recognizes that businesses must frequently move data within and among their corporate entities during normal business operations.

However, the scope of the exemption reflects an asymmetry in the treatment of companies based solely on their legal structure. The proposed rule specifies that a foreign branch of a U.S. company constitutes a U.S. person, even if it is physically present in, subject to the local laws of, and fully staffed by citizens of a country of concern.[12] But a foreign subsidiary of a U.S. company is not offered these protections, and as such is subject to all of the proposed rule's restrictions on companies located in a country of concern. The exemption for corporate group

[11] *Id.* at 86,218.

[12] *Id.* at 86,212-13.

transactions is a welcome step towards remedying this imbalance, but it seems more suited to the situation of a U.S. company with a foreign parent company in a country of concern—where employee data might need to be sent to headquarters for processing—than for legally-distinct foreign branches of domestic U.S. companies.

CTA recommends that DOJ fully rectify this disparity, by broadening the scope of the exemption for corporate group transactions when the foreign entity in a country of concern is the subsidiary of a U.S. parent corporation. This would allow ongoing U.S. oversight and jurisdiction over the treatment of the data without impeding U.S. business operations and inadvertently privileging some corporate structure over others. Internal data-sharing agreements or transfers necessary to a company's business—as distinguished from transfers merely "incidental" to a company's business—should be permitted when the ultimate owner and controller of the data is a U.S. person.

8. DOJ Should Wholly Exempt Data Encrypted in Accordance with CISA Rules

The proposed rule specifies that "bulk U.S. sensitive personal data" is subject to the rule "regardless of whether the data is anonymized, pseudonymized, de-identified, or encrypted."[13] It emphasizes the risks of quantum technologies and other advanced data-processing technologies that may eventually be able to be decrypted or otherwise re-identify such data and declines to accept such measures as sufficient to lift the rule's requirements.

However, the rule specifically requires U.S. persons engaging in restricted transactions to follow security measures promulgated by CISA to prevent covered persons from accessing the relevant data. CISA's requirements specifically mandate a variety of encryption, anonymization, and other similar methods to "protect covered data during the course of restricted transactions." Indeed, CISA's *only* data-level security requirements, other than using "identity and access management techniques to deny authorized access to covered data by covered persons and countries of concern," revolve around the very methods which DOJ says are insufficient to ensure security. At the data level, CISA mandates encryption (Section II.B), data minimization and masking[14]—which it specifically describes as "aggregation, pseudonymization, de-identification, or anonymization"[15]—and other, similar "privacy-enhancing technologies."[16] Indeed, re-identification or de-anonymization of data is not common and is often extremely difficult, and DOJ's cited studies do not offer definitive evidence that re-identification of truly anonymized data is a real risk.

CTA believes that these CISA security measures are well thought-out and reliable, and should be trusted in a broader context. If DOJ likewise believes that these measures will be successful in protecting sensitive U.S. personal data, it should recognize that they are successful in doing so more broadly. CTA therefore recommends that DOJ exclude data that is anonymized and encrypted in accordance with CISA's data-level requirements from the scope of the rule.

---

[13] *Id.* at 86,205.

[14] *See Proposed Security Requirements for Restricted Transactions: E.O. 14117 Implementation*, CISA (Oct. 2024), https://www.cisa.gov/sites/default/files/2024-10/Proposed-Security-Requirements-EO-14117-21Oct24508.pdf, at 4-5.

[15] *Id.* at 5.

[16] *Id.*

9. Restricted Transactions Should Permit Certain Authorized Access to Covered Data by Covered Persons

CTA understands that the NPRM contemplates not only the prohibition of data brokerage transactions with countries of concern altogether, but also the prevention of risks relating to covered persons or countries of concern from *accessing* bulk U.S. sensitive personal data or government data in restricted transactions. However, the NPRM states that the goal of the security measures implemented in restricted transactions is "to address national security and foreign-policy threats that arise when countries of concern and covered persons access government-related data or bulk U.S. sensitive personal data."[17] The goal of restricted transactions, in CISA's words, is to "*mitigate* the risk of sharing bulk U.S. sensitive personal data with countries of concern or covered persons."[18] Neither rule expresses an intention to *prohibit* all access to covered data by any and all covered persons. But the rule as written lends itself to an interpretation that this is its aim in that it primarily discusses the prevention of *access* to any covered data by covered persons, not the prevention of risks arising from that access.

But by definition, restricted transactions involve access to covered data by covered persons. An employment agreement with an individual in a country of concern for a task relating to covered data is pointless if the agreement is permitted only so long as the individual never accesses that data at all. The intent of the security requirements should be to establish conditions under which such restricted transactions might go forward, not to prohibit them entirely. Indeed, CISA's proposed rules reflect the same paradoxical quality by simultaneously requiring that U.S. persons engaged in restricted transactions use "access controls to prevent covered persons or countries of concern from gaining access to covered data, in any form,"[19] while also mandating that such persons process covered data to "minimize the linkability to U.S. person entities before it is subject to access by a covered person or country of concern."[20]

To preserve the utility of restricted transactions, CTA recommends that DOJ clarify that the restrictions in those transactions relate to the risks attendant in allowing covered persons to access covered data, not to permitting this to occur at all. Specifically, we ask that DOJ specify that the security measures for restricted transactions must robustly prevent "unauthorized" access by covered persons.

10. DOJ Should Exclude De-Identified Precise Geolocation Data from the Scope of the Rule Because It Does Not "Relate to an Individual"

Unlike other categories of sensitive personal information listed in the rule, geolocation data is not fundamentally individual. Personal health and financial data, genomic and biometric data, and even covered personal identifiers may be disaggregated or de-linked from individuals, but they necessarily describe those individuals and are capable of being re-linked, precisely because their collection is related to the individual in question. Geolocation data, however, relates only to devices, not to individuals—a point which DOJ recognizes in the NPRM by

---

[17][17] 89 Fed. Reg. 86,116, 86,133 (2024).

[18] Emphasis added.

[19] *Proposed Security Requirements* at 3.

[20] *Id.* at 4.

setting bulk thresholds for every other category with respect to the number of "U.S. persons,"[21] but for precise geolocation data with respect to the number of "U.S. devices."[22]

As a result, de-identified precise geolocation data is fundamentally distinct from "de-identified" personal financial information or genomic data. Without further information about the device in question, there is no way to link geolocation data to an individual—indeed, it may be difficult to link geolocation data to an individual even *with* information about the device, if information about the device's ownership is not included.

Precise geolocation data that has been de-identified would therefore seem to fall into the category of "[p]ublic or nonpublic data that does not relate to an individual,"[23] which is explicitly exempted from the definition of sensitive personal data. However, the lack of a clear definition for data that "does not relate to an individual" means that the rule could be interpreted to control de-identified geolocation data, even though it cannot be linked to a particular U.S. person.

CTA recommends that DOJ offer a definition for the phrase "relate to an individual" to provide clarity on this point. The definition could borrow from the existing definition for the word "linkable," which specifies that an identifier is "not linked or linkable when additional identifiers or data not involved in the relevant covered data transaction(s) would be necessary to associate the identifiers with the same specific person."[24]

11. DOJ Should Clarify the Meanings of Knowledge and Suspicion

CTA has concerns about a few of the terms used to describe U.S. persons' culpability for others' violations of the rule. In two particular instances, we are concerned that there is sufficient ambiguity to significantly affect the scope of the rule's application, and we would like to see sufficient clarity and specificity to allow us a reliable interpretation.

First, in the definitions section, the proposed rule defines a U.S. person to have acted "knowingly" in violation of the rule when they "had actual knowledge of, or reasonably should have known about, the conduct, circumstance, or result."[25] But the rule does not further define the circumstances under which a person "reasonably should have known" about a violation of the rule; only one of the six examples offered after the definition actually involves a "reasonably should have known" standard, and it is one where it would have been very difficult for the U.S. person *not* to have actually known of the violation.[26]

CTA recommends that DOJ eliminate the "reasonably should have known" provision in favor of an "actual knowledge" standard. This would significantly simplify both compliance and enforcement. Alternatively, DOJ could provide further examples to demonstrate when a person "reasonably should have known" about a violation of the rule, and whether this phrase is primarily meant to capture cases where actual knowledge cannot be definitively proven or whether it intends to meaningfully broaden the scope of knowledge involved.

---

[21] 89 Fed. Reg. 86,116, 86,205 (2024).

[22] *Id.*

[23] *Id.* at 86,212.

[24] *Id.* at 86,211.

[25] *Id.* at 86,210.

[26] *Id.* at 86,211.

Similarly, we are concerned that DOJ has insufficiently clarified what it means when it mandates that U.S. persons performing data brokerage transactions with non-covered foreign parties must report to DOJ on "any known or *suspected* violations" of required the contractual provisions.[27] The term "suspected" is never defined anywhere in the rule, and the term appears to be even broader than the "reasonably should have known" proviso discussed above. DOJ's discussion of this mandate describes it as a requirement for U.S. persons to "take reasonable steps to evaluate whether their foreign counterparties are complying with the contractual provisions" mandated by the rule,[28] but this addition creates more questions than it answers: are further "reasonable steps" beyond the reporting requirement implicated? Does "evaluat[ing]" counterparties' compliance require auditing-style ongoing oversight?

CTA is very concerned that this provision and discussion together will leave U.S. entities completely uncertain of the scope of their compliance obligations in non-prohibited data brokerage transactions, or that enforcement will occur on a broader scope than DOJ may intend. CTA therefore recommends that DOJ provide a definition for "known or suspected" violations or otherwise clarify when a U.S. person's reporting obligation triggers and the extent of knowledge the U.S. person must have for this to occur. We also recommend that DOJ clarify that the reporting obligation is the *only* compliance obligation for U.S. persons associated with data brokerage transactions with non-covered parties, and that such U.S. persons are not compelled to maintain ongoing oversight operations with those counterparties.

* * *

Comments Specific to CISA's Request for Comments:

1. CISA Should Consult More Broadly on Risk Management Policies

CTA supports an ex parte process for the CISA security requirements, as when CISA issues regulations. The complexity of CISA's work means that ongoing industry input, not just a single round of comments, is necessary to make sure that this checklist of requirements is not an undue burden on companies engaging in restricted transactions. Rather than prescribing baseline security requirements per se, CISA should be working with DOJ in its proposed rulemaking to identify security concerns and articulate how those could be remediated through risk management policies that use the NIST CSF. Consistent and engaged communication with industry is particularly key in a regulatory regime as detailed and intensive as this one, and CTA requests that CISA engage further with impacted parties before it creates requirements like these—especially when those requirements are automatically enacted through another rulemaking by another agency.

2. The Effects of Anonymization on a "Covered System" and on "Covered Data" Should Be Aligned

[27] *Id.* at 86,214.

[28] *Id.* at 86,130

CISA's definition of a "covered system" expressly notes that a covered system includes "covered data… regardless of whether the data is encrypted, anonymized, pseudonymized, or de-identified." This means that a system remains covered so long as the data remains covered, regardless of data minimization measures, which suggests that data itself remains covered regardless of data minimization measures.

However, in Section II(A)(2), CISA's security measures explicitly mandate that U.S. persons use data minimization strategies "in such a way to [] render it no longer covered data," and suggests anonymization and de-identification as methods by which previously covered data could cease to be covered. This creates a direct contradiction: a covered system must include covered data. Covered data may cease to be covered through anonymization or de-identification. But a covered system includes covered data regardless of whether it is anonymized or de-identified.

CTA recommends that CISA amend the definition of "covered system" to clarify that it includes covered data, regardless of form, only so long as the data remains covered. Once data has undergone the prescribed data minimization strategies, it is no longer covered data; systems including such no-longer-covered data should themselves no longer be covered.

3. CISA Should Extend the Remediation Period

CTA's members are concerned by the brevity of the period in which known exploited vulnerabilities and other vulnerabilities must be remediated. The proposed 14- or 15-day periods (respectively) are too short to function in practice. Standard security practices require remediation in no fewer than thirty days. CTA urges CISA to lengthen each of these requirements to at least 30 days—if not 45—as CISA has proposed to do for other vulnerabilities deemed high severity.

4. CISA Should Clarify and Narrow the Risk Assessment Requirement

While not overwhelming on its own, CISA's requirement for U.S. persons engaging in restricted transactions to conduct and document risk assessments must be viewed in light of the already-extensive audit and reporting requirements imposed on restricted transactions by the DOJ NPRM. Collectively, this creates an enormous compliance burden for companies seeking to perform restricted transactions, which may in practice render them more prohibited than restricted. CTA requests that CISA either eliminate or otherwise mitigate the scale of the effort required.

Additionally, we request that CISA clarify that the risk assessment is not an additional reporting requirement that must be submitted to, or produced upon request for, CISA or DOJ; instead, the purpose of the risk assessment is for internal use and internal security.

5. CISA Should Clarify Critical Language in the Rule

In the rule, CISA uses language that may be interpreted to impose additional, inadvertent requirements. CTA recommends that CISA streamline and clarify the rule in the following ways.

First, the proposed security requirements mention more than one set of standards and references. CTA understands that CISA seeks to create optionality for U.S. persons engaging in restricted transaction and to ensure that the requirements are not overly prescriptive. But we are concerned that some of these references, which have security standards above those of the actual requirements set out by CISA, might be interpreted to impose those higher standards. As

such, we request that CISA remove all references to resources other than the NIST CSF to avoid confusion.

Second, CISA's internal Cybersecurity Performance Goals (CPGs) require a password of significant length if multifactor authentication is not used—but only if such a password is "technically feasible." CTA notes that, while this rule offers the same 16-character password in lieu of multifactor authentication, there is no caveat for feasibility. We therefore recommend that CISA alter this requirement to read: "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 where technically feasible."

Third, CISA's security measures state that the overarching requirement is of mitigation efforts "sufficient to fully and effectively prevent access to covered data by covered persons and/or countries of concern." But even the most sophisticated and effective efforts may never "fully" prevent access. CTA recommends that CISA eliminate the term "fully" from this line.

Finally, Section II(B) instructs U.S. persons engaging in restricted transactions to use "encryption techniques to protect covered data during the course of restricted transactions." CTA is concerned that this language is imprecise. In our view, it would be more precise and effective for the rule to specify the requirement for data encryption in transit and data encryption at rest. In this regard, we recommend that the requirement be amended to read: "Apply encryption techniques to protect covered data in transit and covered data at rest when the covered data is involved in restricted transactions."

6. CISA Should Seek to Prohibit Only Unauthorized Access

The goal of restricted transactions, in CISA's words, is to "*mitigate* the risk of sharing bulk U.S. sensitive personal data with countries of concern or covered persons,"[29] not to *prohibit* all access to covered data by any and all covered persons. The rule as written offers contradictory suggestions on which of these ideas governs. For instance, it simultaneously requires that U.S. persons engaged in restricted transactions use "access controls to prevent covered persons or countries of concern from gaining access to covered data, in any form," but also mandates that companies process covered data to "minimize the linkability to U.S. person entities before it is subject to access by a covered person or country of concern."

CTA requests that CISA modify Section I(B) to clarify that the goal of access controls is to prevent covered persons or countries of concern from gaining "unauthorized access" to covered data and prevent misuse of the covered data by those persons, rather than merely to prevent all covered persons or countries of concern from any "access." CISA should amend the rest of Section I in accordance with this change.

Additionally, since the ultimate goal is to limit authorized access and prevent misuse, CISA should clarify that the measures in the data-level requirements in II offer multiple options for limiting access accordingly. One such option is to prevent all access to covered data by all covered persons; another is to limit authorization. A third is to utilize the techniques in the data-level requirements to render the covered data non-covered and therefore generally accessible by covered persons necessary to the transaction in question. Therefore, the test for whether the

[29] Emphasis added.

risk is sufficiently mitigated should be, not whether the covered person has "access" to covered data, but whether the chosen combination of data-level requirements "sufficiently prevent misuse of the covered data by covered persons." The risk assessment required by I(C) and the chapeau of II should be edited accordingly.

Conclusion

CTA again thanks DOJ and CISA for this opportunity to provide comments on this important regulatory effort. As DOJ works with its interagency partners to review comments in response to the NPRM, CTA stands ready to serve as a helpful resource and looks forward to continued collaboration with DOJ, CISA, and other U.S. government agencies to advance both U.S. national security and economic competitiveness.

Respectfully submitted,

Ed Brzytwa
Vice President of International Trade
Consumer Technology Association

Rachel Nemeth
Senior Director of Regulatory Affairs
Consumer Technology Association