November 29, 2024

Submitted via Electronic Mail to www.regulations.gov

The Honorable Jen Easterly
Director
Cybersecurity and Infrastructure Security Agency
1110 N. Glebe Road
Arlington, Virginia 20598-0630

RE: Comments of ACT | The App Association on CISA Proposed Security Requirements for Restricted Transactions (Docket No. CISA-2024-0029)

In response to its request for public input on the development of security requirements for restricted transactions as directed by Executive Order (E.O.) 14117, "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," ACT | The App Association hereby submits comments to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

The App Association represents thousands of small business innovators and startups in the software development and high-tech space located around the globe.[1] As the world embraces mobile technologies, our members create the innovative products and services that drive the global digital economy by improving workplace productivity, accelerating academic achievement, and helping people lead more efficient and healthier lives. Today, that digital economy is worth more than $1.8 trillion annually and provides over 6.1 million American jobs.[2]

While the global digital economy holds great promise for App Association member companies, our members face a diverse array of challenges when entering new markets. Some of these challenges involve restrictions imposed by potential trading partners. These restrictions, commonly referred to as "trade barriers," reflect in the laws, regulations, policies, or practices that protect domestic goods and services from foreign competition, artificially stimulate exports of particular domestic goods and services, or fail to provide adequate and effective protection of intellectual property rights. These barriers take many forms but have the same net effect: impeding U.S. exports and investment.

[1] ACT | The App Association, *About*, *available at* http://actonline.org/about.

[2] ACT | The App Association, *State of the U.S. App Economy: 2023*, https://actonline.org/wp-content/uploads/APP-Economy-Report-FINAL-1.pdf

The App Association also understands the importance of balancing the benefits of international trade and access to foreign markets with the national security concerns that are implicated by certain types of economic activity. Protecting the privacy and security of Americans' user data is a key concern of our members. We appreciate DOJ's efforts to understand and examine the balance between protecting Americans' privacy and protection from national security threats and maintaining an international trade environment where American small businesses can continue to thrive. We commit to working with DOJ and other stakeholders to strike such a balance. With respect to digital trade, the small business innovators we represent prioritize the following:

- ***Enabling Cross-Border Data Flows:*** The seamless flow of data between economies and across political borders is essential to the functioning of the global economy. Small business technology developers must be able to rely on unfettered data flows as they seek access to new markets.

- ***Prohibiting Data Localization Policies:*** American companies looking to expand into new markets often face regulations that force them and other foreign providers to build and/or use local infrastructure in the country. Data localization requirements seriously hinder imports and exports, reduce an economy's international competitiveness, and undermine domestic economic diversification. Our members do not have the resources to build or maintain unique infrastructure in every country in which they do business, and these requirements effectively exclude them from commerce.

- ***Preserving the Ability to Utilize Strong Encryption Techniques to Protect End User Security and Privacy:*** Global digital trade depends on the use of strong encryption techniques to keep users safe from harms like identity theft. However, some governments continue to demand that backdoors be built into encryption keys for the purpose of government access. These policies jeopardize the safety and security of data, as well as the trust of end users, by creating known vulnerabilities that unauthorized parties can exploit. From a privacy and security standpoint, the viability of an app company's product depends on the trust of its end users.

With respect to CISA's specific proposals, the small business innovators we represent urge CISA to consider the following recommendations:

- We commend CISA for its effort to align the proposed requirements for restricted transactions with existing cybersecurity guidelines, including the NIST Cybersecurity and Privacy Frameworks, as well as CISA's Cyber Performance Goals. App Association members utilize these frameworks to structure their cybersecurity risk management strategies, so pinpointing specific categories within these frameworks that correspond with each proposed requirement is beneficial for understanding how these requirements can be integrated into current risk management programs. Furthermore, we recommend mapping the proposed requirements to ISO/IEC 27001 and controls from NIST SP 800-171,

which would help organizations comprehend how their existing processes and controls can be applied in relation to the new requirements.

Overall, we find that the proposed requirements are sufficiently robust to mitigate risks associated with access to bulk sensitive personal data or government-related information by countries of concern. However, we believe that certain requirements may be excessively prescriptive or challenging to implement effectively in practice.

- System-Level Requirements

    - CISA should incorporate language that allows greater flexibility in applying system-level requirements based on risk assessments. While we appreciate the built-in flexibility for data-level requirements, we believe similar flexibility should be extended to system-level requirements that affect various IT systems. We propose that CISA include a preamble statement that reads: “For any covered system, apply a risk-based approach to implement the following requirements. If your organization finds certain requirements impractical or unfeasible, document the rationale and implement alternative compensating controls to the greatest extent possible.”

    - CISA should also amend its system-level requirements to permit restricted transactions to proceed when risks are adequately mitigated. While we understand that the rule aims to address potential risks from specific transaction types, it is also intended to allow restricted transactions to occur when those risks are properly managed through compliance with the security requirements. The proposed rule states that no U.S. entity may engage in a covered data transaction “unless the U.S. person complies with the security requirements.” CISA further notes that these security requirements are meant to mitigate the risk of sharing bulk U.S. sensitive personal data or government-related data with countries of concern through restricted transactions. We interpret the intent of the DOJ and CISA to mean that covered persons should have access to covered data under certain conditions—namely, when risks have been appropriately mitigated through adherence to security requirements. If covered persons were entirely barred from accessing covered data, the transaction would fall outside the rule’s scope, rendering the security requirements irrelevant.

    - With this in mind, we encourage CISA to revise proposed requirement I.B to specify that organizations must “implement logical and physical access controls to prevent covered persons or countries of concern from gaining unauthorized access to covered data.” This revision ensures that the requirement’s language is precise and does not prohibit all access, but rather ensures that only authorized access is permitted. Adding this term

allows system owners to determine which individuals, including covered persons, can access covered data and under what conditions. This approach facilitates legitimate activities while ensuring sufficient security measures are in place to mitigate associated risks.

- CISA should reconsider the requirement to "remediate known exploited vulnerabilities (KEVs) within 14 calendar days" by eliminating the rigid "14 days" deadline to allow for greater flexibility. While we appreciate that CISA has connected patching requirements to vulnerability severity levels, we are concerned that maintaining the strict 14-day timeline is overly prescriptive across various commercial IT systems and may prove difficult to meet in practice. We also note that such a stringent timeline is unprecedented in the referenced frameworks; neither the CSF 2.0 nor the CPGs include a similar deadline. Although we recognize that CISA has issued Binding Operational Directives (BODs) 22-01 and 19-02 for federal agencies, imposing inflexible deadlines is not feasible across all commercial contexts, especially for complex vulnerabilities or legacy systems, and does not reflect security best practices. At a minimum, CISA should include language in I.3.a indicating that there may be situations where a vulnerability does not pose a risk to the covered system, thereby negating the need for action. The revised requirement could state: "If patching is not feasible, alternative compensating measures must be implemented to the fullest extent possible and commensurate with the risk presented by the vulnerability in the covered system." Finally, CISA should clarify what is meant by "alternative compensating measures." While it is challenging to provide a comprehensive list of acceptable measures, examples with scenario-based use cases would assist organizations in formulating their remediation strategies.

- CISA should modify requirement I.5 to remove references to "any network interfacing with a covered system." While CISA states this should be done "to the maximum extent practicable," this requirement could significantly expand the workload for organizations and complicate implementation. An alternative approach could involve inventorying and assessing the risks of networks interfacing with the covered system without requiring detailed network topologies.

- CISA should adjust requirement I.B.2 by removing the term "immediately." This standard can be challenging to meet from a compliance perspective, given the varying interpretations of when the timeline actually begins.

- CISA should broaden requirement I.B.3 to specify which personnel should be notified of a logging issue and to address additional potential logging issues. Currently, the requirement mandates that "cybersecurity personnel" be notified, which is overly prescriptive. Additionally, the term "disabled" does not encompass the possibility of a system error. We

suggest revising the language to: "...Implement a process to notify relevant personnel when a critical log source, such as an operating system event logging tool, ceases to produce logs."

- Data-Level Requirements

    - Building on the earlier recommendation for CISA to include "unauthorized" to convey its intent to allow restricted transactions to proceed when risks are properly mitigated, we urge CISA to ensure that its data-level security requirements reflect this intended flexibility. We appreciate that CISA has explicitly incorporated flexibility in the data-level requirements, acknowledging that not all practices are suitable for every type of restricted transaction. However, CISA should clarify that the data-level requirements provide U.S. entities with multiple strategies to mitigate risks when executing restricted transactions. The proposed rule identifies six categories of "sensitive personal data" that could be exploited by a country of concern to harm U.S. national security, including for coercion, blackmail, surveillance, espionage, stifling dissent, and tracking individuals. Importantly, these risks arise when such data can be linked to identifiable U.S. individuals or distinct groups.

    - While completely blocking a covered person's access to sensitive data is one method to comply with CISA's proposed requirements, other options may also be suitable for risk mitigation. For example, organizations that employ robust data protection techniques such as data minimization, masking, or strong encryption—methods included in CISA's data-level requirements—can often prevent the identification of individuals. These privacy-enhancing techniques, or other combinations thereof, can reduce risks by making it impossible for a covered person to associate the information with specific individuals. Consequently, the data-level requirements offer organizations multiple options for mitigating the risk of misuse of data accessed through restricted transactions by covered persons or countries of concern, particularly by ensuring that the data is neither linked nor linkable to individuals.

    - While it is evident that companies should have the flexibility to determine which data protection and privacy-enhancing techniques are suitable for their specific business contexts, clarity is needed regarding how CISA will assess whether such practices are deemed "sufficient" in varying scenarios. CISA should clarify how it will evaluate whether an organization is implementing "sufficient" practices to mitigate risks under the data-level security requirements. Although CISA states that "...persons will have some flexibility in determining which combination of data-level requirements are sufficient to address the risks posed based on the nature of the transaction," the guidance lacks clarity on what constitutes "sufficiency" and the criteria CISA will use to evaluate whether an

organization's chosen practices are appropriately tailored to address risk. We encourage CISA to clarify that a risk is sufficiently mitigated when the selected combination of data-level requirements is appropriate to "prevent the misuse of the covered data by covered persons." Sufficiency should not be based solely on whether a covered person or country of concern has access to the data. Consequently, the risk assessment outlined in Part I.C and the introduction of Part II should be amended to include the term "misuse." Additionally, we recommend removing the word "fully" from the same sentence, as it appears to contradict the intention to adopt a risk-based approach. The revised sentence should read: "...is sufficient to effectively prevent the misuse of the covered data by covered persons."

- CISA should revise the first bullet under requirement II.B to state: "Encrypt covered data in a restricted transaction, regardless of type, during bulk transit and storage using industry-standard encryption appropriate to the risk." This wording clarifies that organizations should select encryption standards that are suitably robust.

- CISA should also clarify the second bullet under requirement II.B. Currently, it is unclear whether CISA is implying that the sole acceptable method for transmitting covered data is using TLS 1.2 or higher, or if it is stating that organizations opting to use TLS must use version 1.2 or above. We recommend that CISA clarify this requirement to reflect the latter interpretation.

The App Association appreciates the opportunity to submit these comments to CISA. We are also appending our related comments to DOJ on its linked Proposed Rule, which we request considering of. We stand ready to work with CISA and other stakeholders to protect the privacy and security of all of Americans while maintaining a competitive environment for U.S. businesses and innovators.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

ACT | The App Association
1401 K St NW (Ste 501)
Washington, DC 20005