November 29, 2024

Alicia Smith, Senior Policy Counsel
Cybersecurity and Infrastructure Security Agency (CISA)
U.S. Department of Homeland Security
CISA - NGL Stop 630
1110 N. Glebe Road
Arlington, VA

"Request for Comment on Proposed Security Requirements for Restricted Transactions under Executive Order 14117"

Document ID CISA 2024-0029-001
Docket No. CISA-2024-0029
Submitted via regulations.gov

Dear Ms. Smith,

The National Foreign Trade Council (NFTC) appreciates this opportunity to respond to the publication of "Proposed Security Requirements for Restricted Transactions under Executive Order 14117" ("Proposed Security Requirements"). We note that these Proposed Security Requirements were published in conjunction with the Department of Justice'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" [Docket No. NSD 104]. The Proposed Security Requirements also seek to implement Executive Order 14117 "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern", issued February 28, 2024. We further acknowledge that CISA has stated that the scope of these Proposed Security Requirements is designed to "address the unacceptable risk posed by restricted transactions, as identified by the Attorney General." Per E.O. 14117 Sec. 2(d) and CISA does not intend for these to be all-inclusive of cybersecurity risks or otherwise reflect a comprehensive cybersecurity program.

NFTC acknowledges the importance and supports the objectives of these Proposed Security Requirements to further implement E.O. 14117 and to address data privacy vulnerabilities and risks associated with bulk data brokerage as well as to deter and prevent the ability of malign foreign actors to access bulk sensitive personal data and U.S. government-related data. We raise here specific concerns regarding system-level and data-level security requirements. We respectfully submit recommendations to strengthen national security objectives and support broader public policy interests.

System-level security requirements

NFTC urges CISA to revise system-level security to harmonize such requirements with the intent of the proposed rule, which is to enable restricted transactions to move forward when their risk can be sufficiently mitigated.

By definition, restricted transactions involve access to covered data by covered persons. The intent of the security requirements is to establish conditions under which such restricted transactions might go forward, not to prohibit them entirely. In CISA's own words, "[t[he security requirements are designed to mitigate the risk of sharing bulk U.S. sensitive personal data or U.S. government related data with countries of concern or covered persons through restricted transactions." Accordingly, CISA must modify its **system-level requirement** (Part I.B) to prevent covered persons or countries of concern from gaining "unauthorized access" to covered data and make corresponding changes to other portions of the requirements (aside from Part II, discussed below). Such changes would harmonize the requirement with the intent of the rule by ensuring that countries of concern and covered persons are not able to access any covered data beyond that which they are authorized to access.

Under the proposed rule, no U.S. person may engage in a covered data transaction "unless the U.S. person complies with the security requirements [promulgated by DHS]." (§ 202.401(a).) A transaction is "covered" (and restricted) if it "involves any access" to covered data by a covered person. (§ 202.210.) We believe the DOJ intended that the Proposed Security Requirements enable access to covered data by covered persons under certain and specific circumstances. Therefore, if covered persons never have access to any covered data whatsoever, the transaction would no longer be "covered" by the rule and none of the security requirements would be necessary. Adding the word "unauthorized" before access would accomplish the intent of ensuring covered systems are sufficiently secure that system owners can regulate which persons, including covered persons, have access to covered data and under what conditions.

CISA's Proposed Security Requirements state that companies shall maintain a regularly updated inventory of covered system assets with each system's respective internet protocol (IP) address (including IPv6). For hardware, this should also include MAC address. (NIST CSF 2.0 ID.AM-01, CISA CPGs 1.A). NFTC notes that this requirement is technically unrealistic. With cloud-based systems, IP and MAC addresses are commonly dynamically assigned, especially as services are dynamically expanded or contracted based on load. Moreover, these IP addresses may not represent the actual public location those resources are accessed by (with load balancers, gateways, and other solutions providing intermediate processing). **NFTC recommends implementing requirements to inventory systems based upon whatever unique system or infrastructure identifiers that make sense within context rather than anachronistic and non-static identifiers.**

In Part I.B.3.a, CISA proposes to require storage of all log data for twelve months. This may not be feasible in every circumstance. NFTC understands the need to retain logs for a sufficient length of time to aid in investigations based on the volume and detail of the logs and urges CISA to develop realistic parameters that can be implemented by companies across sectors. **NFTC recommends the following alternative language: Data should be held for twelve months minimally however certain types of logs such as full network traffic may not be able to be stored for that length of time.**

Data-level requirements

NFTC seeks clarification regarding the intent of data-level security requirements and harmonization of these requirements with the intent of DOJ's proposed rule. CISA should also further clarify that the Data Level Requirements (Part II) offer a flexible set of options for U.S. persons that engage in restricted transactions to mitigate the risks of access to such data by countries of concern or covered persons by sufficiently de-identifying the data.

DOJ's proposed rule identifies six categories of "sensitive personal data" that could be exploited by a country of concern to harm U.S. national security. Adversaries may misuse this data for various activities, including

coercion, blackmail, surveillance, espionage, curbing dissent, and tracking targets. Such risks arise when such data is linked or linkable to any identifiable U.S. individual or to a discrete and identifiable group of U.S. persons. Denying access to all covered data by covered persons is one way to comply with the rule. But as the other components of Part II suggest, if sufficiently strong data minimization, data masking, encryption, or other privacy enhancing techniques are deployed, the risks of access to covered data by covered persons may be sufficiently minimized, because the covered person would be incapable of linking the data to individual persons.

Data-level requirements offer a combination of options to mitigate the risk that covered data accessed by a country of concern or a covered person through a restricted transaction could be misused by taking steps to ensure the data is neither linked nor linkable to individuals. (It would remain "covered data" under the rule because "Bulk U.S. Sensitive Personal Data" includes data regardless of whether the data is "anonymized, pseudonymized, de-identified, or encrypted.")

NFTC recommends that the appropriate test for whether the risk is sufficiently mitigated should be whether the chosen combination of data-level requirements "sufficiently prevent misuse of the covered data by covered persons" rather than whether a covered person has "access" to covered data. The risk assessment required by Part I.C, and the chapeau of Part II, should also be edited accordingly.

About NFTC

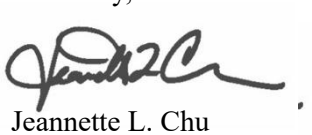
The NFTC, organized in 1914, is an association of U.S. business enterprises engaged in all aspects of international trade and investment. The NFTC supports open, rules-based trade, including a level and competitive playing field. Our membership covers the full spectrum of industrial, commercial, financial, and service activities. Our members value the work of the Departments of Homeland Security and Treasury, and other agencies, in implementing E.O. 14117 to protect bulk sensitive data and U.S. government-related sensitive data from malign foreign actors.

Our goal is always to strengthen U.S. industries and their global supply chains and to help protect national security and economic security interests. Robust trade relationships are central to economic and national security. NFTC's National Security Policy Initiative brings the voice of business to policymakers on global security issues affecting international trade. Companies play a vital role in promoting American values, including human rights and democracy. Our data-driven recommendations support American competitiveness and technology leadership, which are central to our national security.

Thank you again for this opportunity to comment on CISA's Proposed Security Requirements for implementing E.O. 14117 in conjunction with DOJ's proposed rule, "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons."

We welcome the opportunity to discuss this important matter and answer any questions that you may have regarding these comments or recommendations. I can be reached at (202) 887-0278 or at jchu@nftc.org.

Sincerely,



Jeannette L. Chu
Vice President for National Security Policy