November 26, 2024

Submitted electronically via Regulations.gov
Director Jen M. Easterly
Cybersecurity and Infrastructure Security Agency
Department of Homeland Security
1110 N. Glebe Road
Arlington, VA 20598-0630

Re: Federal Register No. 2024-24709
Security Requirements for Restricted Transactions Under Executive Order 14117

Dear Director Easterly:

The Securities Industry and Financial Markets Association ("SIFMA"), Futures Industry Association ("FIA") and Institute for International Bankers ("IIB") appreciate the opportunity to comment on the proposed rulemaking concerning the Security Requirements for Restricted Transactions Under Executive Order 14117.

Commentors

SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association ("GFMA").

FIA is the leading global trade organization for the futures, options and centrally cleared derivatives markets, with offices in Brussels, London, Singapore and Washington, D.C. FIA's membership includes clearing firms, exchanges, clearinghouses, trading firms and commodities specialists from about 50 countries as well as technology vendors, law firms and other professional service providers. FIA's mission is to support open, transparent and competitive markets; protect and enhance the integrity of the financial system; and promote high standards of professional conduct.

IIB represents the U.S. operations of internationally headquartered financial institutions from more than 35 countries around the world. The membership consists principally of international banks that operate branches, agencies, bank subsidiaries, and broker-dealer subsidiaries in the United States. The IIB works to ensure a level playing field for these institutions,

which are an important source of credit for U.S. borrowers and comprise the majority of U.S. primary dealers. These institutions also enhance the depth and liquidity of U.S. financial markets and contribute significantly to the U.S. economy through direct employment of U.S. citizens, as well as through other operating and capital expenditures.

Background

As you are aware, on February 28, 2024, President Biden announced an Executive Order ("EO") 14117 directing the Department of Justice ("DOJ") to promulgate regulations that restrict or prohibit transactions involving certain bulk transfers of sensitive personal data or United States Government-related data to countries of concern or covered persons.[1] As directed by the EO, on March 5, 2024, the DOJ published in the Federal Register an Advance Notice of Proposed Rulemaking ("ANPRM") regarding "Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern."[2] Following the ANPRM, on October 29, 2024, the DOJ published in the Federal Register a Notice of Proposed Rulemaking regarding "Provisions Pertaining to Preventing Access to U.S. Sensitive Personal Data and Government-Related Data by Countries of Concern or Covered Persons."[3] In tandem with the DOJ's Notice of Proposed Rulemaking, the Cybersecurity and Infrastructure Security Agency ("CISA") published a Notice of Proposed Rulemaking ("NPRM") proposing security requirements for restricted transactions in the DOJ's Notice of Proposed Rulemaking.[4]

Our members conduct thousands of data transfers every hour, completing transactions on behalf of millions of investors around the globe. As such, these rules will have a significant impact on how our members conduct business and, as a result, how millions of Americans access the financial markets. Therefore, it is critical that CISA, in finalizing its rule, use precise language to ensure the financial services industry is not unduly burdened. We respectfully submit that our recommendations below comport with the ANPRM's aspiration to "carefully calibrate" the enhancement of national security while "minimizing disruption to commercial activity."[5]

As the EO lays out, CISA must publish certain security requirements for restricted transactions. The EO, however, does not prescribe the specific requirements except that they must be based on "the Cybersecurity and Privacy Frameworks developed by the National Institute of

---

[1] Exec. Order No. 14,117, Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern, 89 Fed. Reg. 15421 (Feb. 28, 2024), *available at* https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related [hereinafter EO].

[2] National Security Division; Provisions Regarding Access to Americans' Bulk Sensitive Personal Data and Government-Related Data by Countries of Concern, 89 Fed. Reg. 15780 (proposed Mar. 5, 2024), *available at* https://www.federalregister.gov/documents/2024/03/05/2024-04594/national-security-division-provisions-regarding-access-to-americans-bulk-sensitive-personal-data-and [hereinafter ANPRM].

[3] National Security Division; 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. 86116 (proposed Oct. 29, 2024), *available at* https://www.federalregister.gov/documents/2024/10/29/2024-24582/provisions-pertaining-to-preventing-access-to-us-sensitive-personal-data-and-government-related-data.

[4] Department of Homeland Security; Request for Comment on Security Requirements for Restricted Transactions Under Executive Order 14117, 89 Fed. Reg. 85976 (proposed Oct. 29, 2024), available at https://www.federalregister.gov/documents/2024/10/29/2024-24709/request-for-comment-on-security-requirements-for-restricted-transactions-under-executive-order-14117 [hereinafter NPRM].

[5] 89 FR 15782.

Standards and Technology." As such, CISA has significant leeway to develop requirements to ensure national security, but not to unduly burden lawful transactions. Both the EO and the DOJ's Notice of Proposed Rulemaking make clear that financial transactions need special considerations and exemptions so as not to add regulatory cost and burden to the economy and the U.S. financial markets. We believe that the CISA NPRM should do the same.

Under various federal, state or foreign financial institution regulatory regimes as may be applicable to any given financial institution, including but not limited to the Gramm-Leach-Bliley Act's ("GLBA") Safeguards Rules, the New York State Department of Financial Services' ("DFS") Cybersecurity Regulation (23 NYCRR 500), the Federal Reserve Board's ("FRB") guidelines for managing cybersecurity risk, and the EU Digital Operational Resilience Act ("DORA"), financial institutions must already adhere to strict and comprehensive cybersecurity measures for protecting their systems and information under their possession or control. These regulations, by sector-specific regulators, are generally consistent with the NIST frameworks, and reflect a focus on the particular data protection issues relevant to the financial services industry. Adding a new generic set of restrictions, even though based on some of the same sources, could have the effect of creating confusion, unnecessary work to navigate similar standards, and potentially conflicting technical direction. As such, we recommend CISA consider any entity that is subject to applicable financial sector cybersecurity requirements to be in compliance with the proposed security requirements in the NPRM as a matter of deemed substitute compliance. This would accomplish the same goals that the proposed security requirements set out to accomplish, and removes the need for financial institutions to comply with potentially duplicative or conflicting generic security requirements.

We are particularly concerned about the application of these security requirements because they seem to be a statement of generic cybersecurity practices, but not targeted to the national security threat that is being addressed by the DOJ's Notice of Proposed Rulemaking. The security requirements proposed are broad requirements that are not at all tailored to ensuring covered persons that are parties to restricted transactions do not gain unauthorized access to data. Some requirements are particularly burdensome and attenuated from the risk the requirements are supposed to address, such as certain privacy requirements, comprehensive risk assessments, and documentation requirements. Moreover, the rulemaking does not address the potential costs of these measures in light of the national security benefits to be achieved, and it does not address the relative cost or effectiveness of these controls in relation to each other. Without guidance as to the relative effectiveness and priority of controls, companies are left with a mere list of controls without an underlying evaluation of the relative cost or benefit of these controls. We believe that any security requirements proposed beyond compliance with those security regimes already applicable to entities in the financial services industry should be targeted to specific risks that arise from restricted transactions, not a mix of disconnected best practices. The benefits of implementing them should also outweigh the costs. Therefore, we recommend that the proposed security requirements first be able to be met by compliance with existing regulatory regimes, and that any stricter proposed controls be directly tied to cybersecurity risks from the restricted transactions as intended by the EO and subject to financial services entities' ability to alternately implement compensating controls consistent with the risk-based approach permitted by the existing regulatory framework.

* * * * * *

We appreciate your consideration of this request. If you have questions or would like to discuss these comments further, please reach out to Melissa MacGregor at mmacgregor@sifma.org.

Sincerely,

Melissa MacGregor
Deputy General Counsel &
Corporate Secretary
SIFMA

Allison Lurton
General Counsel &
Chief Legal Officer
FIA

Stephanie Webster
General Counsel
IIB