Title: The "Protecting Americans' Data from Foreign Adversaries Act" and DOJ "Data Security Program" – Important Updates

Brief Overview: In April 2024, the PADFAA was signed into law as part of a broader national security package that makes it unlawful for data brokers to sell or transfer "personally identifiable sensitive data" of U.S. persons to entities that are controlled by foreign adversaries, primarily China, Russia, Iran, and North Korea. On February 28, 2024, Former President Biden issued Executive Order 14117 directing the DOJ to establish the DSP with regulations that both implement and expand upon the PADFAA. In early 2025, the DSP regulations were finalized with the Final Rule published on January 8, 2025, effective on April 11, 2025.

This advisory addresses several issues which entities and individuals should immediately consider, including who is affected, the types of data and transactions that are covered, the countries identified as foreign adversaries, prohibited vs. restricted transactions, compliance requirements, and enforcement and penalties.

Authors: Jodutt M. Basrawi (basrawi@clm.com), Jenny Frank (frank@clm.com), Jack Griem (griem@clm.com) , Matthew D. Dunn (mdunn@clm.com)

Practice Area: Cybersecurity & Data Privacy

Full Article:

As of April 11, 2025, the Department of Justice (the "DOJ") issued its Data Security Program (the "DSP") Compliance Guide, which aims to assist entities and individuals to navigate the complex compliance requirements of the Protecting Americans' Data from Foreign Adversaries Act (the "PADFAA") and the DSP. These comprehensive federal controls are intended to minimize the risk that foreign adversaries can access, use, and exploit U.S. government data and bulk sensitive personal data of Americans, and include substantial penalties for violations. Individuals and entities that do business in or with certain foreign counties need to be well aware of these requirements and immediately ensure compliance. While the Federal Trade Commission, tasked with enforcing the penalties for violations of the PADFAA, has not yet brought any enforcement actions, recent comments by Commissioner Melissa Holyoak indicate that the FTC will prioritize enforcement of the PADFAA during this administration.

Background

In April 2024, the PADFAA was signed into law as part of a broader national security package that makes it unlawful for data brokers to sell or transfer "personally identifiable sensitive data" of U.S. persons to entities that are controlled by foreign adversaries, primarily China, Russia, Iran, and North Korea. On February 28, 2024, Former President Biden issued Executive Order 14117 directing the DOJ to establish the DSP with regulations that both implement and expand upon the PADFAA. In early 2025, the DSP regulations were finalized with the Final Rule published on January 8, 2025, effective on April 11, 2025. The PADFAA prohibits certain actions related primarily to data brokers and the DSP broadens the set of data transactions with enhanced data security controls, comprehensive compliance obligations, and details definitions,

procedures, and enforcement mechanisms. Thus, the PADFAA and DSP mark the most significant federal data security restrictions in over two decades.

This advisory addresses several issues which entities and individuals should immediately consider, including who is affected, the types of data and transactions that are covered, the countries identified as foreign adversaries, prohibited vs. restricted transactions, compliance requirements, and enforcement and penalties.

Who Is Affected?

These regulations affect two primary categories of entities: data brokers and other organizations that collect data directly from individuals (e.g., first-party data holders). Data brokers are subject to the strictest rules, such as an outright ban on selling covered types of data to foreign adversaries. Penalties for any willful violations of this regulation are severe and include both civil fines and criminal charges. Other businesses and companies that collect data directly from individuals have more nuanced obligations that require such organizations to assess any foreign exposure of personally identifiable sensitive data that they hold and store. If an organization engages in data transfers that could potentially provide foreign adversaries with access to protected data, then the organization must determine if such access is covered under the DSP as either prohibited or restricted.

Covered Data Types

The PADFAA and the DSP apply to personally identifiable sensitive data on a large scale and certain U.S. government-related data. As such, an organization that sells or transfers applicable types of covered data needs to implement data protection policies that should include detailed explanatory information about the handling, storage, and transfer of the following categories:

- Personal Identifiers: information that is traceable to specific individuals;
- Biometric Identifiers: e.g., fingerprints, facial recognition data, iris scans, DNA profiles;
- Genetic Information: human genomic data;
- Precise Geolocation Data: data that indicates an individual's location with a high degree of accuracy;
- Personal Health Data: e.g., medical histories, health conditions, genetic test results;
- Personal Financial Data: e.g., financial account information, transaction histories, credit reports;
- Social Media and Communications Content: e.g., posts, messages, browsing history; and
- Government Personnel and Security Data: information about U.S. government employees or sensitive government operations.

Additionally, the PADFAA and the DSP establish category-specific volume thresholds to determine what constitutes 'bulk' data, including personal financial data of more than 10,000 U.S. persons and personal identifiers collected on more than 100,000 U.S. persons.

Foreign Adversaries and Covered Persons

The PADFAA and the DSP specifically enumerate a defined set of nations deemed to be foreign adversaries or countries of concern. Under the PADFAA, the core "Foreign Adversary Countries" (or "Countries of Concern") are China, Russia, Iran, and North Korea. Under the DSP and as referenced in Executive Order 14117, additional "Countries of Concern" include Cuba and Venezuela. Notably, the definition of entities "controlled by" these countries is broad, covering companies incorporated or headquartered in these countries as well as any companies with more than 20% ownership by foreign adversaries.

In addition, covered persons include foreign individuals that are employees of a Country of Concern or entities headquartered or incorporated in such countries or 50% owned by such countries. The definition also encompasses any person subject to the direction or control of a foreign person or entity from these countries, as well as foreign individuals who are citizens or residents of a Country of Concern. Furthermore, entities in which foreign individuals from Countries of Concern serve as officers, directors, or in senior management positions are covered, along with subsidiaries and affiliates of entities headquartered in these countries, regardless of where the subsidiary itself is incorporated. The regulations also capture entities acting as agents, representatives, or at the direction of a Country of Concern, and any entity that has entered into joint ventures, partnerships, or significant commercial arrangements with entities from Countries of Concern where such arrangements could provide access to covered data or technology. Notably, the DSP grants authority to add additional countries or entities to the list based on national security assessments, providing flexibility to address emerging threats.

Prohibited vs. Restricted Transactions

The regulations distinguish between prohibited transactions and restricted transactions that are permitted if specific conditions are satisfied. Prohibited transactions include instances in which data brokers sell or transfer certain covered types of data, such as personally identifiable sensitive data to foreign adversary-controlled entities and transfers of U.S. human genomic data to any foreign adversaries. Restricted transactions are permitted so long as designated security measures are incorporated and implemented, including Vendor or Service Provider Agreements (e.g., U.S. companies using cloud services or IT providers supplied by foreign adversaries); Employment Agreements (e.g., work contracts with individuals hired in foreign adversary countries who could obtain access to covered types of sensitive data); and Investment or Partnership Agreements (e.g., arrangements with foreign adversary investors who will likely have access to covered types of sensitive data).

Compliance Requirements

All applicable businesses and companies must implement comprehensive compliance programs to adhere to the requirements of the PADFAA and the DSP, including the following:

- "Know Your Data" Program: data mapping and risk assessments to identify which types of covered data an organization collects and holds, where such covered data is stored and transmitted, and who (both internally and externally) has access to such covered data;

- U.S. Cybersecurity and Infrastructure Security Agency (CISA) Security Requirements: to prevent or mitigate the risk of restricted transactions, organizations must implement CISA-defined cybersecurity and data protection measures, including strong encryption methods, anonymization or pseudonymization techniques to minimize individual identification, access controls limiting data to minimal authorized personnel, enhanced network security standards with ongoing improvements, and tested and verified incident response plans;

- Documentation and Certification: maintaining written policies that outline the explicitly identified compliance required under the PADFAA and the DSP, testing the efficacy and thoroughness of risk assessments, confirming third-party due diligence records for reliability and accuracy, evaluating relevant contracts to ensure the inclusion of sufficiently protective and risk-mitigating clauses, and periodically updating and improving personnel training programs and documenting training reports;

- Auditing and Monitoring: conduct routine audits of data flows and vendor relationships, test data and network systems to prevent and mitigate the occurrence of any prohibited transfers, and monitor regulatory updates to confirm uninterrupted compliance; and

- Record-Keeping and Reporting: keep all records, logs, files, and documentation related to data transactions for covered types of data for the entire duration of the required retention period, immediately report all unauthorized access incidents or attempts, and consider voluntary self-disclosure of violations. According to DOJ guidance, the National Security Division of the DOJ may consider a qualifying voluntary self-disclosure as a mitigating factor in any enforcement action.

Enforcement and Penalties

Both the PADFAA and the DSP regulations carry significant penalties for non-compliance. Civil penalties can include up to $53,088 per violation under PADFAA (enforced by the FTC), or up to the greater of $368,136 per violation or twice the value of the underlying transaction under the DSP (enforced by the DOJ). Criminal penalties are reserved for willful or knowing violations, especially in relation to aiding foreign governments. The DOJ's National Security Division is responsible for enforcement efforts and coordinates with the FBI for investigations. While the DOJ built in a "good faith compliance" grace period for organizations actively working to comply with the regulations, this is still not a free pass for continued non-compliance because the grace period is meant to encourage organizations to get their compliance programs in order quickly but remains a finite duration of time. Any egregious or deliberate violations will be enforced immediately and are not subject to the benefits of the grace period.

Suggested Action Items

Businesses and companies that handle bulk amounts of U.S. personally identifiable sensitive data or government-related data, particularly if the circumstances involve any movement of covered types of data across borders, should undertake the following:

1. Conduct an Emergency Data Flow Audit by mapping all data flows, especially including data crossing U.S. borders; identifying any connections with foreign adversaries; and flagging high-risk data transfers for immediate remediation.

2. Address Critical Non-Compliance by terminating or modifying any clearly prohibited data arrangements; implementing interim controls for identified restricted transactions; and updating the organization's internal policies and external third-party contracts with sufficient compliance clauses.

3. Develop a Comprehensive Compliance Program by establishing formal "Know Your Data" processes.

4. Implement CISA Security Requirements for any restricted transactions.

5. Create Reporting and Documentation Systems and Mechanisms for record-keeping purposes and maintain accurate logs of information for the required retention periods.

6. Incorporate Training and Procedures for relevant staff and personnel with access to covered types of data pursuant to the PADFAA and the DSP requirements.

7. Seek Advisory Opinions as needed by requesting guidance from the DOJ for uncertain cases and documenting all decision-making processes and responses.

Conclusion

The PADFAA and the DSP impose significant restrictions on many individuals and entities involved in industries and transactions involving U.S. government data and bulk sensitive personal data. With enforcement of these regulations now effective, immediate action is essential to ensure compliance. Our team stands ready to assist in navigating these complex requirements efficiently and effectively. Please contact us to discuss your organization's distinct situation and develop an individually tailored and detailed compliance strategy.

* * *

This article was written by **Jodutt M. Basrawi** (212-238-8767, basrawi@clm.com), **Jennifer L. Frank** (212-238-8650, frank@clm.com), **Matthew D. Dunn** (212-238-8706, mdunn@clm.com), and **John M. Griem, Jr. (**212-238-8659, griem@clm.com) of Carter Ledyard & Milburn LLP.

* * *

the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.