February 28, 2024

Alert: Executive Order on Preventing Access to Americans' Bulk Sensitive Data and Government-Related Data

by Jon Neiditz

Late today the White House issued its Executive Order significantly enhancing the protection of Americans' bulk sensitive personal data from access by countries deemed as threats. It establishes a comprehensive framework to safeguard categories of personal information deemed sensitive against exploitation and unauthorized access by foreign entities identified as countries of concern. Although this initiative does indeed set forth measures to prevent the misuse of sensitive data on a global scale, its impact on the private sector will generally be felt through data broker arrangements, vendor agreements, employment agreements, and investment agreements, rather than through mitigation of the massive data breaches that have been the primary pipeline of sensitive information to hostile governments.

1. Scope and Definitions

Types of Data Protected:

The Executive Order delineates "sensitive personal data" as information, to the extent consistent with applicable laws such as sections 203(b)(1) and (b)(3) of the International Emergency Economic Powers Act (IEEPA), which includes:

- Covered personal identifiers
- Geolocation and related sensor data
- Biometric identifiers
- "Human 'omic data" (including genomic, epigenomic, proteomic, transcriptomic, microbiomic, metabolomic data)
- Personal health data
- Personal financial data

This data, either alone or in combination, is deemed to pose a risk to United States national security if it is linked or linkable to any identifiable U.S. individual or a discrete and identifiable group of U.S. individuals.

Countries of Concern:

A "country of concern" is defined within the Executive Order as any foreign government identified by the Attorney General (through specific criteria set in the Order) that:

- Has engaged in a long-term pattern or serious instances of conduct significantly adverse to the national security of the United States or the security and safety of U.S. persons.
- Poses a significant risk of exploiting bulk sensitive personal data or U.S. Government-related data to the detriment of the national security of the United States or the security and safety of U.S. persons.

We know from statements of senior administration officials -- but not from the Executive Order -- that the countries of concern now include China, Russia, North Korea, Iran, Cuba and Venezuela.

2. Prohibitions and Restrictions

Specific Prohibitions on Data Transactions with Identified Threats:

The Executive Order imposes stringent prohibitions and restrictions on transactions involving sensitive personal and government-related data with countries of concern. It mandates the development of regulations that will:

- Prohibit or restrict U.S. persons from engaging in transactions that involve bulk sensitive personal data or U.S. government-related data when such transactions pose an unacceptable risk to national security.
- Target transactions that may enable countries of concern or covered persons to access sensitive data in ways that contribute to the national emergency described in the order.
- Apply to transactions initiated, pending, or completed after the effective date of the regulations, ensuring that new and ongoing data handling practices comply with the Order's security objectives.

Restrictions on Data Handling and Transfer Processes:

The Order outlines a framework for identifying prohibited and restricted transactions, emphasizing:

- The need for clear classifications of transactions that pose security risks.
- The development of security requirements and enforcement guidance to mitigate risks associated with restricted transactions.
- A process for licensing exceptions, ensuring that certain necessary transactions can proceed under strict oversight.
- The establishment of recordkeeping and reporting obligations to support enforcement and regulatory efforts.

The Executive Order tries to ensure that the regulatory framework does not unduly hinder legitimate commercial activities and necessary data flows, so that issue will constitute a major part of your review of the standards promulgated.

3. Government Roles and Responsibilities

Enforcement and Oversight:

Key responsibilities include:

- **The Secretary of Homeland Security, through the Cybersecurity and Infrastructure Security Agency (CISA)**, is tasked with proposing, seeking public comment on, and publishing security requirements aimed at addressing the unacceptable risks posed by restricted transactions. These security measures will be based on the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology (NIST).
- **The Attorney General**, in coordination with the Secretary of Homeland Security (through CISA), will issue enforcement guidance regarding these security requirements. This collaborative approach ensures that the enforcement of the Executive Order is grounded in the latest cybersecurity and privacy standards, enhancing the effectiveness of the measures put in place to protect sensitive data.

Process for Identifying and Addressing Risks:

The Executive Order establishes a structured process for identifying and addressing risks associated with foreign access to sensitive data. This includes:

1. **Developing Security Requirements**: Leveraging expertise from CISA and guided by NIST's frameworks, to create robust security protocols for transactions deemed to pose a risk.
2. **Issuing Enforcement Guidance**: To ensure consistent and effective application of the security requirements, with a focus on mitigating risks from countries of concern.
3. **Public Engagement**: Inviting public comment on proposed security measures to incorporate a wide range of perspectives and expertise in the final regulations.

4. Compliance Requirements for Businesses

Detailed Guidance on Compliance Measures:

Businesses handling sensitive personal data must adhere to compliance measures specified in the Executive Order, including:

- **Implementing Security Requirements**: Organizations are required to follow security requirements proposed by the Secretary of Homeland Security, through the Cybersecurity and Infrastructure Security Agency (CISA), in coordination with the Attorney General. These requirements are to be grounded in the Cybersecurity and Privacy Frameworks developed by the National Institute of Standards and Technology (NIST).
- **Adhering to Enforcement Guidance**: The Attorney General, in coordination with CISA, will issue enforcement guidance regarding the security requirements, ensuring businesses understand the standards they need to meet.

Recommendations for Adjusting Data Processing and Protection Practices:

- **Rule, Regulation, and Standard Adherence**: Businesses must adjust their data processing and protection practices to comply with rules, regulations, standards, and requirements promulgated by the Secretary of Homeland Security, in coordination with the Attorney General.
- **Interpretive Guidance Compliance**: Organizations should stay informed about and comply with any interpretive guidance issued, aiding in the interpretation and application of the established security requirements.

5. Exemptions and Balancing

Exemptions Related to Financial Services and Essential Operations:

- The Order expressly avoids imposing generalized data localization requirements that would mandate the storage of Americans' bulk sensitive personal data or U.S. Government-related data within the United States or require computing facilities processing this data to be located within the U.S.
- It also refrains from broadly prohibiting U.S. persons from engaging in commercial transactions, including the exchange of financial and other types of data as part of commercial goods and services sales, with entities and individuals in countries of concern. This decision is made to avoid disrupting the substantial consumer, economic, scientific, and trade relationships the U.S. maintains with other nations.

Balance Between Data Protection and Information Flow:

- The Order aims to restrict access by countries of concern to sensitive data that could threaten national security, while still supporting an open, global, interoperable, reliable, and secure Internet.
- It emphasizes the importance of protecting human rights online and offline, supporting a vibrant global economy through cross-border data flows essential for international commerce and trade, and facilitating open investment.
- To ensure that the U.S. continues to meet these policy objectives, the Order is implemented in a manner that calibrates national security restrictions to minimize risks without unduly disrupting commercial activity or the global flow of data. It asks that any regulations and actions taken under the Order to specifically address the national security threat posed by access to sensitive data by countries of concern, thus maintaining a balance between securing sensitive information and preserving vital data flows.

6. Implementation Timeline and Expectations

Timeline for Regulatory Actions and Compliance Deadlines:

Within **180 days** of the Executive Order's date, the Attorney General, in coordination with the Secretary of Homeland Security and in consultation with the heads of relevant agencies, is tasked with publishing the proposed rule for notice and comment. This rule is expected to:

- Identify classes of transactions deemed prohibited due to their risk to national security.
- Specify classes of transactions for which established security requirements sufficiently mitigate risks, thus categorizing them as restricted but permissible under certain conditions.

- Determine and list countries of concern along with classes of covered persons subject to the Executive Order.
- Develop mechanisms for providing clarity to affected persons, including designations of covered persons and decisions regarding licensing.
- Establish a licensing process for transactions that might otherwise be prohibited or restricted, allowing for modification or rescission of licenses in concordance with input from relevant U.S. departments and agencies.

Expectations from Businesses and Government Entities in the Implementation Phase:

- Businesses and government entities are expected to closely monitor the development of these rules and prepare to adjust their operations in accordance with the new requirements. This preparation includes assessing current transactions and partnerships involving sensitive personal data to identify potential areas of concern.
- Entities must also stay informed about the identification of countries of concern and covered persons, as these designations will directly impact permissible transactions.
- Organizations should prepare to engage with the new licensing process, particularly if their operations involve transactions that may fall under the prohibited or restricted categories but are deemed essential for business continuity.
- Throughout this period, it is crucial for affected parties to contribute to the notice and comment process, offering insights that could shape the final regulations in a manner that balances national security needs with the practicalities of international commerce and data flow.

7. Action Items

To ensure compliance with the Executive Order, organizations should take the following steps:

1. **Review Current Data Practices**: Assess and document the handling, storage, and transfer of sensitive personal data to identify any practices that may need adjustment to comply with the new requirements.
2. **Identify Potential Risk Areas**: Determine if any ongoing or planned transactions, including contracts with data brokers, third-party vendor agreements, employment agreements and investment agreements, could involve countries of concern or covered persons as defined by the Executive Order.
3. **Update Data Security Measures**: Align data protection practices with the security requirements proposed by the Secretary of Homeland Security, based on the Cybersecurity and Privacy Frameworks developed by NIST.
4. **Monitor Regulatory Developments**: Stay informed about the publication of proposed rules, identification of countries of concern, and any updates on restricted or prohibited transactions.
5. **Prepare for the Licensing Process**: If your business operations involve transactions that may be classified as restricted or prohibited, begin preparing to engage with the newly established licensing process.
6. **Contribute to Public Comment**: Participate in the public comment process for the proposed rule to ensure that industry perspectives and concerns are considered in the final regulations.

7. **Implement Compliance Training**: Educate your staff about the changes in regulations and the importance of compliance, focusing on those directly involved in handling sensitive data.
8. **Develop an Incident Response Plan**: Ensure you have a robust plan in place for responding to data breaches or compliance inquiries, including clear communication channels and protocols for engaging with U.S. government agencies.