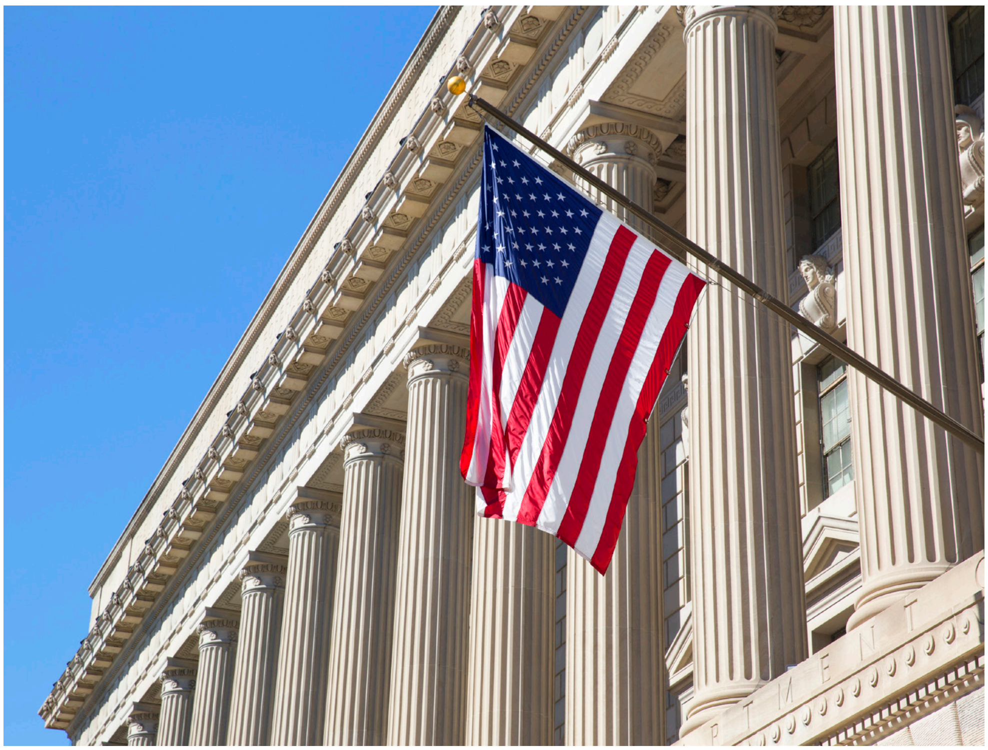
BDO KNOWS:

TRANSACTION ADVISORY SERVICES



CONTACT

JOHN E. LASH
Director National Security Compliance / CFIUS
202-644-5417 / jlash@bdo.com

KEVIN BEYER
Senior Manager National Security Compliance / CFIUS
214-259-1484 / kbeyer@bdo.com

NAVIGATING NATIONAL SECURITY REGULATIONS IN THE DATA ECONOMY

Dynamic compliance strategies have become an imperative in deal consideration for foreign direct investment (FDI) in critical infrastructure as the United States seeks to modernize the Committee on Foreign Investment in the United States (CFIUS) review process, protect national security from emerging risk, and maintain an open investment policy. The rapidly shifting global economy, disruptive innovation, dual-use technologies, and the weaponization of information have become an unrelenting combination of force stimulating change and creating risk as billions of dollars of foreign investment surge into the U.S. economy.

With high level of investment comes high-value targets, and presently, there are few resources considered as valuable as data. Data, coupled with current sophisticated analytical and manipulation techniques, allows companies to extract even more value from that underlying information thereby changing the risk profile of the transaction. The growth of technology and innovation have led to a necessary evolution in how national security risks are evaluated.

A key risk component in the CFIUS process evaluates whether the transaction would expose personally identifiable information (PII) of a U.S. person—including genetic information, protected health information (PHI), geographic movement, or other sensitive data. The data economy has exasperated risk relative to PII and PHI of U.S. persons, particularly if the company with access and control of such information becomes the target of a foreign acquisition. In order to assess national security risk of a proposed transaction, parties must recognize the threat, vulnerability, and consequences of exploitation of data as a direct result of the transaction.

Understanding the Data Threat

Data quantity and quality in the advent of the Internet of Things (IoT) era, have made data an immensely valuable resource. Traditional computing devices (e.g., personal computers, tablets, cell phones) are no longer the only appliances accessing on-line data and/or storing data. Items such as wearable technology, smart appliances, and biometric applications are now utilized to access and/or store data and can become potential entry points for malicious activity, further increasing the complexity of logical security—in short, who can access information and what is the potential consequence if that information is exploited are no longer simple questions to answer.

Information exploitation, or the ability to weaponize information, has significantly increased risks associated with cross-border transactions. Consequently, CFIUS' level of scrutiny of transactions involving foreign direct investment in the U.S. has expanded to consider both the intent and capabilities of the acquirer as well as the value of the data collected. Companies regularly focus efforts on the protection of IP, sensitive competition and trade information, and privacy regulations; however, as the vulnerabilities evolve for the raw data in certain industrial sectors, a shift in compliance strategy is essential.

Data Rich Industrial Sectors

Specific sector exposure exists within the broad industries of financial services and healthcare—focusing on collection, storage, and access to data and information. Financial services companies possess a wealth of information, including but not limited to: U.S. customer personally identifiable information, U.S. company non-public financial information, U.S. government customer PII, and law enforcement sensitive information. Extensive customer vetting is performed at financial institutions as it relates to Know Your Customer (KYC) and Enhanced Due Diligence (EDD) on both individual U.S. customers as well as U.S. businesses—including required cooperation with U.S. Lawful Process Requests. In many cases, the data contained within the financial services sector provides a mosaic theory view of the institutions' U.S. customer industrial base.

Within the healthcare sector—from medical equipment manufacturers to insurers to medical service providers—the complexities of collecting and protecting patient information is an industry in and of itself.

These companies possess protected health information (PHI) that relates not only to past, present, or future physical or mental health/genetic conditions, but also payment provisions, geographic identifiers, and other underlying patient information, which could be analyzed to establish patterns or trends that create risk to U.S. public health and safety.

Identifying the potential threat in a company's own information, how that information may be a national security vulnerability, and then recognizing and mitigating the potential risk profile of the transaction is integral in evaluating deal metrics in data rich industrial sectors.

Intelligent (Information) Warfare

The ability to utilize technological advances to establish new-generation artificial intelligence (AI) to leverage raw data and support command and decision making, enhance military education, upgrade defense equipment, and establish other military/civil fusion activities has created a paradigm shift in data vulnerability.

Weaponizing information via AI or alternative data manipulation techniques facilitates the ability for controlling entities to engage in malicious activities against the United States that may have adverse effects that ultimately impact national security. The ability to identify key U.S. personnel, perform social network link analysis, geospatial or temporal analysis, or to establish mosaic interpretations related to U.S. public health and safety critical assets creates data threats that must undergo a risk-based assessment model review during the consideration of a transaction.

If these threats are persistent in the transaction, companies should consider their mitigation options to first ensure national security remains intact and secondarily evaluate the commercial reasonableness of the transaction with consideration to potential mitigation or divestiture of certain U.S.-nexus assets.

Mitigating Data Risk

Successful mitigation strategies can be key to transactions with pervasive data threats as a direct result of foreign direct investment. First and foremost, these strategies must alleviate the national security concerns of the transaction in an efficient, effective, and verifiable way.

Mitigation of data and information threats in a transaction may include compliance requirements specifically targeted towards "access to" and "storage of" certain types of information—whether that information is considered sensitive information, personally identifiable information (PII), protected health information (PHI), or end-user information. An additional item for consideration is original source code as often times source code will have access to, transmit, and store such information.

Companies should recognize what, how, and where information is collected, stored, and transmitted both domestically and internationally—as well as how, where, and by whom that information may be accessed. Mitigation terms tend to be robust pertaining to collection and storage of U.S. citizen data and foreign entity ability to access and/or control such information.

BDO National Security Compliance Pillars

As a practical point, it is recommended that companies evaluate their critical data and information using the following guidelines:

- **Foundational Accountability:** Assess relevant controls, compensating controls, policies, procedures, and processes that were either created, amended, or already in place specific to compliance requirements under the mitigation terms
- **Compliance Practices—Mitigation Term Project Quality, Criticality, and Completeness:** Evaluate the effectiveness of the current state of compliance or the program for facilitating compliance with the mitigation terms negotiated with CFIUS
- **Target State Architecture—Logical and Physical:** Assess the conceptualization, development, and deployment of technical controls capable of providing a defense-in-depth security posture as it relates to the integrity, reliability, and responsiveness of the organization
- **Operational Control Deployment:** Evaluate the controls that have been deployed in the operational environment and provide a validation of the implementation, maintenance, and remediation of such controls—including both technical and human capital instances
- **Database Reliability:** Assessment of the availability, completeness, auditability, and integrity of enterprise-wide compliance efforts
- **Site Visits:** Evaluation of physical and logical security features of key sites – such as data centers, network operation centers, closed facilities, and backup centers which store or provide access to protected information
- **CFIUS Compliance Optimization:** Establishing guidance on compliance strategy and operational implementation of controls with respect to any identified gaps in compliance or risk areas as it relates to mitigation items. Ensure the ability to monitor or audit against the mitigated activities to provide reasonable assurance to the U.S. Government that the activities effectively mitigate national security risks identified

Compliance Strategy

Organizations must recognize the potential national security implications of a proposed transaction at the onset of the deal—performing a risk based assessment and evaluating the consequence of any exploitation of a national security vulnerability. As the threat landscape continues to evolve through technological innovation, the advent of the data economy, and the weaponization of information—companies should ensure national security compliance is an essential component of any cross-border investment strategy.