CFIUS Cybersecurity Services

An intelligence-led, expert-driven, strategic approach to global cybersecurity challenges affecting your organization – your people, your operations, and your reputation.

The Committee on Foreign Investment in the United States (CFIUS) gained significant strength following the passage of the Foreign Investment Risk Review Modernization Act (FIRRMA) in 2018. FIRRMA expanded CFIUS authority to review and restrict foreign investments on national security grounds, meaning that foreign-backed U.S. businesses with sensitive technologies or large amounts of personally identifiable information could be on the receiving end of heightened government oversight and investigation. FTI Cybersecurity works with parties pursuing a deal to assess cybersecurity maturity and ensure CFIUS compliance expectations are met.

CFIUS CYBERSECURITY SERVICES

Program and Data Assessment: Assessments allow FTI Cybersecurity to determine your organization's unique vulnerabilities and evaluate if your business is aligned with best practices and CFIUS standards. Our team will ensure your organization has properly protected its controlled unclassified information and International Traffic in Arms Regulation data, and will determine if you meet industry standard best practices, such as those outlined in NIST 800-171/171a. We will identify and assess your vulnerabilities and devise a holistic set of scored recommendations, helping secure your company's future.

Gap Remediation: After conducting assessments and due diligence, our experts work with your organization to remediate any gaps found within your system, or anything that would cause your organization to fall outside the CFIUS cybersecurity standards.

Transaction Services: The cybersecurity and IT aspects of M&A transactions have become one of the most pervasive, complex, risky and, at times, expensive activities to address. Our cybersecurity experts work throughout the transaction lifecycle, delivering due diligence; integration synergy assessments, roadmaps and program management; and carve-out planning, transition (TSA) management, and buy-side and sell-side support. We proactively address vulnerable organizational areas to improve security and send a message of accountability to an acquiring or targeted company in an M&A.

HOW WE CAN HELP

The way in which parties in a cross-border deal manage their cybersecurity is highly relevant to the scrutiny CFIUS can exercise under its extended authority. Not only are new deals subject to these investigations, but also those in the past; CFIUS reviews non-notified transactions from previous years that in some cases have led to penalties. Here are primary cybersecurity actions parties must take to align with CFIUS guidelines:

- Conduct a regulatory gap assessment to identify necessary changes that need to be made to achieve compliance across export controls, data privacy, and cybersecurity obligations
- Assess the data environment, the control status of any sensitive technology, security infrastructure, and existing cybersecurity policies, procedure, and processes
- Design a control development and revision strategy that will recommend technology solutions, human resources protocol, and policy changes uninterrupted.

RELATED OFFERINGS

Independent Assessorship

An independent security program assessment that determines the effectiveness of an organization's risk management capabilities is often a necessity due to regulatory requirements.

We have extensive experience with assessorships across a variety of environments and risk profiles, including in scenarios involving government regulated entities. Specifically, our team has assisted organizations with the development, design, implementation, and testing of security policies, processes, and technology assessments to achieve compliance.

We have performed numerous security program risk assessments, including analyzing internal risk and compliance monitoring capabilities, program management and governance capabilities, and individual product, process, and system-based security controls. Through this experience designing and conducting assessments, we are able to accurately outline the steps needed to enhance and sustain improvement efforts, helping organizations meet regulatory demands.

Cyber Readiness

We work with your team to evaluate your specific needs to tailor solutions that enhance security and readiness to defend against the unique cybersecurity risks facing your organization. Being ready for cyber threats is fundamental to the success of your incident response program. We work with your business to select and implement controls to limit the number of potential incidents your organization may face.

Vulnerability Assessment

We design custom vulnerability assessment plans to ensure your infrastructure is secure and stable, preventing hackers from infiltrating systems with unidentified and unpatched vulnerabilities. Regular assessments allow our team to test systems for any irregularities, inconsistencies, and anomalies that might render an organization's network vulnerable to attack.

Due Diligence

Cybersecurity & IT

We identify and report current cybersecurity and IT strengths, weaknesses, and threats, as well as future opportunities and requirements to reduce risks and costs, improve capability and service delivery, and add enterprise value. We deliver tailored reports, from high-level "red flag" risk assessments to deep thesis-based analyses, with value-creation recommendations and one-time and run-rate cost models.

Third-Party

Data shared with third-party vendors can leave organizations vulnerable to exposure and also creates another access point for hackers to exploit. Our experts perform third-party due diligence assessments to analyze their cyber risk, and provide tailored recommendations for how to mitigate any threats.

Complex Investigations

Our team routinely tackles global, large-scale, and complex issues, that often stem from data privacy related concerns, and demand intricate solutions. We quickly unearth key facts and data sets to enable timely and strategic decisions in investigations, leading to cutting-edge and data-driven results. This is particularly relevant as CFIUS shifts its focus from reviewing notified transactions to researching non-notified transactions from previous years.

Litigation Support

Our team supports clients facing high-stakes litigation, including class action data privacy cases, arbitration and compliance investigations, and regulatory scrutiny. We help clients protect their enterprise value through expert witness testimony; evidence collection, handling, and preservation; and forensic analysis and complex modeling.

CFIUS Beyond Cybersecurity

Cybersecurity plays a big role in CFIUS regulations. For additional assistance in CFIUS matters, our experts in the Export Controls, Sanctions & Trade practice can help with export classifications, mitigation agreement compliance, and overall assistance with export control compliance and other post-transaction matters.

Why FTI Cybersecurity

Multidisciplinary Expertise

Intelligence-led, expert-driven, strategic approach to cybersecurity challenges

Core team from intelligence agencies, law enforcement, prosecuting offices, and global private sector institutions

Globally Positioned

Ability to respond anywhere in the world

Ability to staff the largest and most complex engagements and investigations

Relationships with the top global intelligence agencies, regulatory authorities, and private agencies

Integrated & Comprehensive

No other firm in the space has a crisis communications practice

Integration of FTI Consulting's expertise across the platform

1982

Year Founded and $6.2B equity market capitalization*

50/100

Advisor to 50 of the top 100 Private Equity International (PEI) firms

7,700+

Employees

NYSE:FCN

Publicly traded

99/100

Advisor to 99 of the world's top 100 law firms

82

82 of Fortune Global 100 corporations are clients

**Number of total shares outstanding as of April 20, 2023, by the closing price per share on April 20, 2023.*

ANTHONY J. FERRANTE
Global Head of Cybersecurity
Senior Managing Director
+1 202 312 9165
ajf@fticonsulting.com

JORDAN RAE KELLY
Head of Cybersecurity, Americas
Senior Managing Director
+1 202 312 9140
jordan.kelly@fticonsulting.com

DAVID DUNN
Head of Cybersecurity, EMEA & APAC
Senior Managing Director
+44 7816 251410
david.dunn@fticonsulting.com

05242023 | FTI Cyberse