Insider Risk, National Security, and the Limits of U.S. Legal Frameworks:

A Critical Analysis of CMMC and Protection Mechanisms in the Age of Chinese Cyber Espionage

By: Kenneth Vignali

JM Student, George Mason University

December 2025

Table of Contents

Abstract

I. Introduction

II. Background and Problem Statement

III. Case Studies Highlighting Insider Risk

IV. Legal Frameworks Governing Insider Risk

V. Gaps in Current Frameworks

VI. Comparative Perspective: Chinese Legal Architecture

VII. Proposed Legal and Policy Reforms

VIII. Conclusion

Abstract

Insider risk within the United States Defense Industrial Base has evolved into a complex phenomenon driven by globalized development pipelines, cloud-centric architectures, and distributed subcontractor labor. While traditional insider threat doctrine focused on malicious employees acting within the physical boundaries of U.S. contractor facilities, modern insider risk[1] arises from structural conditions involving foreign nationals, offshore developers, cloud administrators, identity-federated personnel, and supply chain actors who possess legitimate access to systems containing sensitive or controlled information.

This paper argues that the Defense Industrial Base faces a modern category of insider risk that is not limited to intentional wrongdoing by trusted employees. Instead, insider risk must be understood as a structural condition shaped by three intersecting forces: the globalization of technical labor, the architecture of cloud and identity management systems, and the legal obligations imposed on foreign nationals by their home governments.[2] Collectively, these factors create access pathways that adversarial nations can exploit without relying on traditional insider placement or long-term recruitment.

Drawing from verified case studies including the DOJ indictments of PRC-affiliated actors, congressional scrutiny of Microsoft's cybersecurity failures before the House

[1]See generally NAT'L INSIDER THREAT TASK FORCE, NATIONAL INSIDER THREAT POLICY AND MINIMUM STANDARDS FOR EXECUTIVE BRANCH INSIDER THREAT PROGRAMS (2012).

[2]See Zhonghua Renmin Gongheguo Guojia Qingbao Fa [National Intelligence Law of the People's Republic of China] art. 7 (promulgated by the Standing Comm. Nat'l People's Cong., June 27, 2017, effective June 28, 2017).

Committee on Homeland Security,[3] the DHS Cyber Safety Review Board's findings on the Storm-0558 intrusion,[4] and the July 2025 ProPublica investigation revealing Microsoft's decade-old "digital escorts" program that permitted Chinese engineers to help maintain DOD cloud systems with minimal U.S. supervision,[5] this paper demonstrates that adversaries increasingly leverage contractor ecosystems to gain insider-level access. It further analyzes China's National Intelligence Law, Data Security Law,[6] and Counter-Espionage Law, which collectively compel Chinese nationals and companies to assist state intelligence services, thereby creating unavoidable insider-risk vectors in U.S. supply chains.

This paper advances a central argument: while the United States possesses multiple statutory and regulatory tools, including the Computer Fraud and Abuse Act ("CFAA"), the Economic Espionage Act ("EEA"), the Espionage Act, Section 889 of the National Defense Authorization Act ("NDAA"), and the Cybersecurity Maturity Model Certification ("CMMC"),[7] these mechanisms inadequately address modern insider risk. Most critically, existing criminal statutes operate only after harm has occurred, punishing individual bad actors but placing no preventative burden on government contractors themselves. The only

[3]A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security: Hearing Before the H. Comm. on Homeland Sec., 118th Cong. (June 13, 2024) [hereinafter Cascade of Security Failures Hearing].

[4]CYBER SAFETY REVIEW BD., U.S. DEP'T OF HOMELAND SEC., REVIEW OF THE SUMMER 2023 MICROSOFT EXCHANGE ONLINE INTRUSION 2 (2024).

[5]Renee Dudley, A Little-Known Microsoft Program Could Expose the Defense Department to Chinese Hackers, PROPUBLICA (July 15, 2025, 5:00 am), https://www.propublica.org/article/microsoft-digital-escorts-pentagon-defense-department-china-hackers.

[6]Zhonghua Renmin Gongheguo Shuju Anquan Fa [Data Security Law of the People's Republic of China] (promulgated by the Standing Comm. Nat'l People's Cong., June 10, 2021, effective Sept. 1, 2021).

[7]32 C.F.R. pt. 170 (2024).

tools that impose prospective obligations on contractors are rigorous CMMC enforcement and, potentially, application of 18 U.S.C. § 793(f)'s gross negligence standard to digital safeguarding failures. Without these enforcement mechanisms, contractors face minimal accountability for structural vulnerabilities in their supply chains.

This paper concludes by proposing statutory reforms, regulatory action under DoD authority, and enhanced CMMC insider-threat requirements. It argues that U.S. law must evolve to treat insider risk not as an incidental compliance matter, but as a core national-security imperative requiring integrated legal, technical, and organizational safeguards.

I. Introduction

Insider threats have historically been a persistent challenge to national security, but in the twenty-first century, their significance has expanded as the lines between physical espionage and cyber operations have blurred. At its core, "insider risk" encompasses malicious insiders who act with deliberate intent, negligent insiders whose careless conduct facilitates compromise, and compromised insiders who are coerced or manipulated by foreign adversaries. Unlike purely external threats, these risks exploit the trust relationship inherent in access to sensitive data and systems, making detection and mitigation uniquely difficult.

What distinguishes modern insider risk from its traditional counterpart is the structural transformation of the Defense Industrial Base itself. Contractors increasingly depend on distributed software development teams across multiple continents, subcontractor personnel in foreign jurisdictions, cloud service providers whose internal staff possess privileged access, identity federation and single-sign-on systems that authenticate users outside the organizational boundary, offshore development and testing environments connected to U.S. repositories, and third-party vendors contributing code or administrative

support. All of these developments create new vulnerabilities that traditional security frameworks were not designed to address.

The United States finds itself at an inflection point in addressing these structural vulnerabilities. This paper argues that the Defense Industrial Base faces a modern category of insider risk that is not limited to intentional wrongdoing by trusted employees. Instead, insider risk must be understood as a structural condition shaped by three intersecting forces: the globalization of technical labor, the architecture of cloud and identity management systems, and the legal obligations imposed on foreign nationals by their home governments, particularly China's National Intelligence Law, which compels all citizens and organizations to "support, assist, and cooperate with state intelligence work."

This paper advances three central claims. First, insider risk is underregulated relative to its scope, leaving gaps that adversaries systematically exploit. Second, while CMMC offers a promising compliance regime, its structure underemphasizes behavioral and legal mechanisms for insider prevention, relying heavily on self-attestation that sophisticated vendors can game. Third, and most critically, the existing statutory framework operates almost entirely as an ex-post punishment mechanism: the CFAA, EEA, and Espionage Act criminalize individual misconduct after the fact but impose virtually no prospective burden on contractors to prevent structural vulnerabilities. The only mechanisms that require contractors to take preventative action are rigorous CMMC enforcement and potential application of 18 U.S.C. § 793(f)'s gross negligence standard. Without these enforcement tools, the legal framework amounts to symbolic deterrence rather than substantive safeguard.

The discussion proceeds as follows. Part II provides background on how global development ecosystems and foreign legal systems create structural insider risk. Part III presents case studies demonstrating national security implications, including the Microsoft

digital escorts program and Storm-0558 intrusion. Part IV surveys legal frameworks: the CFAA, EEA, Espionage Act, Section 889, and CMMC. Part V identifies enforcement gaps these frameworks leave unaddressed. Part VI compares U.S. approaches to China's mandatory intelligence cooperation laws. Part VII advances comprehensive reforms organized by implementing authority and prioritized by criticality. Part VIII concludes with reflections on why only CMMC enforcement and § 793(f) application provide meaningful leverage to impose preventative obligations on contractors.

II. Background and Problem Statement

The Defense Industrial Base historically relied on domestic workforces operating within secured facilities, with well-defined personnel security requirements[8] and limited external access pathways. Today, the structure of defense technology development has changed dramatically. Modern defense contractors operate within a globalized ecosystem where code is written in multiple countries, cloud infrastructure is managed by multinational corporations, and supply chains extend through layers of subcontractors whose personnel are often invisible to prime contractors and government oversight alike.

At the same time, adversarial foreign governments have created statutory regimes that compel their citizens and domestic companies to support intelligence activities. China's National Intelligence Law,[9] Data Security Law, and Counter-Espionage Law impose mandatory cooperation requirements that apply extraterritorially. This creates a structural asymmetry: U.S. law relies on voluntary compliance and after-the-fact prosecution, while Chinese law guarantees that any Chinese national with access to U.S. defense systems faces

[8]See NAT'L INDUS. SEC. PROGRAM OPERATING MANUAL (NISPOM), DOD 5220.22-M (Feb. 28, 2006).

[9]National Intelligence Law, supra note 2.

legal compulsion to cooperate with state intelligence services, whether or not that individual harbors malicious intent.

The term "embedded" as used throughout this paper refers to foreign nationals placed within U.S. contractor organizations through legitimate employment or subcontracting relationships. These individuals receive authorized access to sensitive systems by virtue of their employment. They may work remotely or be physically present in U.S. facilities, yet simultaneously face legal obligations under foreign law, particularly China's National Intelligence Law, to cooperate with state intelligence agencies. This creates unavoidable structural risk: an individual may be both a trusted insider from the contractor's perspective and a potential intelligence asset for an adversarial government, regardless of personal intent.

The problem addressed in this paper is that U.S. law and policy have not yet adapted to these realities. The Espionage Act,[10] the Economic Espionage Act,[11] the CFAA,[12] DFARS 252.204-7012,[13] NIST SP 800-171,[14] and CMMC[15] all provide meaningful safeguards, but none fully address structural insider risk arising from foreign legal compulsion, global supply chain labor, cloud privilege pathways, or identity federation. As a result, U.S. contractors may comply fully with existing requirements and still remain vulnerable to foreign intelligence exploitation. More fundamentally, these frameworks do not require contractors to

[10]18 U.S.C. §§ 792-798 (2018).

[11]18 U.S.C. §§ 1831-1839 (2018).

[12]18 U.S.C. § 1030 (2018).

[13]DFARS 252.204-7012 (2023).

[14]NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-171 REV. 2, PROTECTING CONTROLLED UNCLASSIFIED INFORMATION IN NONFEDERAL SYSTEMS AND ORGANIZATIONS (2020).

[15]Cybersecurity Maturity Model Certification (CMMC) Program, 89 Fed. Reg. 90,362 (Nov. 15, 2024) (to be codified at 32 C.F.R. pt. 170).

take proactive steps to mitigate structural risks; they merely punish individuals who commit crimes.

III. Case Studies Highlighting Insider Risk

A. Microsoft's Digital Escorts Program

A stark illustration of structural insider vulnerability emerged in July 2025 when a ProPublica investigation revealed Microsoft's decade-old "digital escorts" program, which had allowed Chinese engineers to help maintain the Defense Department's computer systems with minimal supervision by U.S. personnel.[16] Under this arrangement, U.S. citizens with security clearances served as intermediaries between China-based Microsoft engineers and the Pentagon's cloud infrastructure, manually inputting commands into military systems on behalf of their foreign counterparts who were barred from direct access.

The investigation found critical weaknesses in this model. Many escorts lacked the technical expertise to evaluate the code they were entering, raising concerns that they could unwittingly introduce vulnerabilities or malicious scripts into sensitive government networks.[17] As one current escort told ProPublica: "We're trusting that what they're doing isn't malicious, but we really can't tell." Job postings for escort positions advertised pay starting at $18 per hour, with the primary prerequisite being a valid security clearance rather than software engineering expertise. The program was so low-profile that even the Defense Information Systems Agency had difficulty finding anyone familiar with it.

[16]Dudley, supra note 5.

[17]Id.

The national security implications were immediately recognized by former intelligence officials. Harry Coker, former senior executive at the CIA and NSA and former National Cyber Director during the Biden administration, stated: "If I were an operative, I would look at that as an avenue for extremely valuable access. We need to be very concerned about that." He added that he and his former intelligence community colleagues "would love to have had access like that."[18] John Sherman, who served as Chief Information Officer for the Department of Defense during the Biden administration, said he was "surprised and concerned" and that he "probably should have known about this," calling for "a thorough review by DISA, Cyber Command and other stakeholders."[19]

The disclosure prompted immediate action. Defense Secretary Pete Hegseth announced that the use of Chinese nationals to service DOD cloud environments was terminated effective immediately and initiated a review to ensure no similar programs existed elsewhere in the Defense Department.[20] Microsoft announced it would end the use of China-based engineers to support its cloud services for the Defense Department.[21] Senator Tom Cotton, Chairman of the Senate Intelligence Committee, wrote to Secretary Hegseth warning that "DOD must guard against all potential threats within its supply chain, including those from subcontractors."[22]

---

[18]Id. (quoting Harry Coker, former senior executive at the CIA and NSA and former National Cyber Director).

[19]Id. (quoting John Sherman, former Chief Information Officer for the Department of Defense).

[20]Press Release, U.S. Dep't of Def., Pentagon Halts Chinese Coders Affecting DOD Cloud Systems (Dec. 2025).

[21]Natalie Alms, Microsoft Ends Use of China-Based Engineers to Patch DOD Systems, NEXTGOV/FCW (July 18, 2025).

[22]Letter from Sen. Tom Cotton, Chairman, S. Select Comm. on Intelligence, to Pete Hegseth, Sec'y of Def. (July 18, 2025).

Yale Law School's Jeremy Daum explained that Chinese laws allow government officials to collect data "as long as they're doing something that they've deemed legitimate," and that the digital escort arrangement presents an opening for espionage "whether it be putting someone who's already an intelligence professional into one of those jobs, or going to the people who are in the jobs and pumping them for information." He noted that "it would be difficult for any Chinese citizen or company to meaningfully resist a direct request from security forces or law enforcement."[23] David Mihelcic, DISA's former Chief Technology Officer, assessed the risk bluntly: "Here you have one person you really don't trust because they're probably in the Chinese intelligence service, and the other person is not really capable."[24]

This case demonstrates that structural insider risk is not theoretical. A major defense contractor operated a program for nearly a decade that created direct access pathways for foreign nationals subject to mandatory intelligence cooperation laws, supervised by personnel lacking the technical expertise to detect malicious activity, all while ostensibly complying with government contracting requirements. The digital escorts case illustrates the central failure this paper addresses: existing legal frameworks allowed this vulnerability to persist because they impose no affirmative duty on contractors to prevent structural insider risk, only to refrain from individual criminal acts.

B. The Storm-0558 Intrusion and Congressional Scrutiny

Congressional scrutiny of Microsoft's cybersecurity practices intensified following the summer 2023 Microsoft Exchange Online intrusion by Storm-0558, a Chinese state-

[23]Dudley, supra note 5 (quoting Jeremy Daum, Senior Research Fellow, Paul Tsai China Center at Yale Law School).

[24]Id. (quoting David Mihelcic, former DISA Chief Technology Officer).

sponsored threat actor. In June 2024, the House Committee on Homeland Security convened a hearing titled "A Cascade of Security Failures: Assessing Microsoft Corporation's Cybersecurity Shortfalls and the Implications for Homeland Security." The Department of Homeland Security Cyber Safety Review Board (CSRB) had concluded that Storm-0558 accessed Microsoft Exchange accounts using authentication tokens signed by an inactive private encryption key that Microsoft created in 2016, obtaining tens of thousands of individual U.S. government emails by compromising accounts of officials working on national security matters relating to China.

Chairman Mark Green characterized the intrusion as exploiting "basic, well-known vulnerabilities that could have been avoided through basic cyber hygiene," emphasizing that the intrusion "was not sophisticated" but rather "avoidable."[25] Ranking Member Bennie Thompson noted that the CSRB found Microsoft's security culture "inadequate" and requiring "an overhaul," and that Microsoft provides an estimated 85 percent of the productivity software used by the federal government.[26] Microsoft President Brad Smith accepted responsibility for each finding in the CSRB report and testified that the company was implementing its Secure Future Initiative with "the equivalent full-time of 34,000 engineers" working on what he described as "the largest engineering project focused on cybersecurity in the history of digital technology."[27]

Significantly, the hearing also addressed Microsoft's operations in China and the implications of China's National Intelligence Law. Representative Carlos Gimenez

[25]Cascade of Security Failures Hearing, supra note 3 (statement of Chairman Mark Green).

[26]Id. (statement of Ranking Member Bennie Thompson).

[27]Id. (statement of Brad Smith, Vice Chair and President, Microsoft Corporation).

questioned Smith directly about Microsoft's compliance with the 2017 law requiring all organizations and citizens to cooperate with China's intelligence agencies. Smith claimed Microsoft does not comply with such requests and stated that "there are two types of countries in the world, those that apply every law they enact and those that enact certain laws, but don't always apply them." Representative Gimenez responded skeptically, noting that based on his work on the Select Committee on China, "all companies in China have to cooperate with the intelligence agencies of China and the People's Liberation Army."[28] This exchange illustrates the fundamental tension between global technology operations and foreign intelligence cooperation requirements that creates structural insider risk. Microsoft's position that China simply does not enforce its intelligence cooperation laws strains credulity given the well-documented patterns of Chinese state-sponsored cyber operations.

These two Microsoft-related incidents, the digital escorts program and the Storm-0558 intrusion, reveal that even sophisticated technology vendors with significant government contracts can fall short of adequate security practices. More importantly, they demonstrate that compliance with existing regulatory frameworks does not prevent structural vulnerabilities. Microsoft presumably satisfied DFARS requirements and whatever CMMC certifications applied to its government contracts, yet these frameworks failed to prevent either the decade-long operation of the digital escorts program or the authentication key mismanagement that enabled Storm-0558. This pattern underscores the paper's central argument: without rigorous enforcement mechanisms that impose affirmative duties on contractors, legal frameworks become compliance exercises rather than substantive safeguards.

[28]Id. (statement of Rep. Carlos Gimenez, Member, H. Comm. on Homeland Sec.).

IV. Legal Frameworks Governing Insider Risk

A. The Computer Fraud and Abuse Act (CFAA)

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, has historically served as the primary federal statute criminalizing computer-related misconduct. The statute prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access and thereby obtain[ing]...information from any protected computer."[29] For decades, prosecutors used the CFAA's "exceeds authorized access" provision to pursue insider threats, arguing that employees who misused their legitimate access for unauthorized purposes violated the statute.

The Supreme Court's 2021 decision in *Van Buren v. United States*[30] dramatically narrowed the CFAA's utility for addressing insider threats. The case involved a police officer who accepted payment to query a law enforcement database for personal gain using his valid credentials. The Court adopted a narrow "gates-up-or-down" interpretation, holding that "exceeds authorized access" refers only to accessing areas of a computer system one lacks permission to enter, not using permitted access for improper purposes.[31] The Court reasoned that a broader interpretation would criminalize a wide range of commonplace computer activity and extend CFAA liability far beyond its intended scope.[32]

This creates critical gaps in addressing modern insider threats. Under the *Van Buren* holding, individuals who are compromised by foreign intelligence services or who never had

[29]18 U.S.C. § 1030(a)(2)(C) (2018).

[30]Van Buren v. United States, 593 U.S. 374 (2021).

[31]Id. at 391-92.

[32]Id. at 387-88.

benign intent are not covered by the CFAA simply because the contractor authorized their access, even though access was not granted for malicious purposes. In the context of Chinese contractors or subcontracted coders, an insider could insert malicious code or exfiltrate sensitive data without violating the CFAA so long as access itself was authorized, regardless of how that access was used. The digital escorts case illustrates this gap: Chinese engineers with authorized access could potentially exfiltrate information or introduce vulnerabilities without triggering CFAA liability because their access was formally authorized through the escort program.

Thus, while the CFAA remains symbolically significant as the primary computer crime statute, *Van Buren* has diminished its practical value for combating insider threats in national security contexts. More fundamentally, even before *Van Buren*, the CFAA operated exclusively as an ex post mechanism: it punished individual criminals after they committed prohibited acts but imposed no obligation on contractors to prevent insider access vulnerabilities. The statute provides no basis for requiring contractors to vet subcontractor personnel, restrict offshore development, or implement structural safeguards against foreign intelligence exploitation.

B. The Economic Espionage Act (EEA)

The Economic Espionage Act, 18 U.S.C. §§ 1831-1839, was enacted in 1996 to criminalize theft of trade secrets, with particular focus on foreign espionage. Section 1831 targets theft intended to benefit foreign governments: "Whoever, intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly...steals, or without authorization appropriates, takes, carries away, or conceals...a

trade secret" faces criminal penalties.[33] Section 1832 addresses theft for private or commercial advantage.

The EEA has been used in high-profile insider cases, including *United States v. Aleynikov*,[34] where a Goldman Sachs programmer was charged with stealing proprietary source code. Although Aleynikov's conviction was later overturned because the source code did not qualify as a "product" under the then-existing EEA definition, the case led to statutory amendments expanding EEA coverage to include intangible property and products. The case illustrates how insiders in technical roles can exfiltrate intellectual property with profound implications for national security and economic competitiveness.

In practice, the EEA offers a more direct pathway than the CFAA to prosecute malicious insiders acting on behalf of foreign adversaries. Yet the statute faces significant limitations. First, proving "intent to benefit" a foreign government under § 1831 requires a high evidentiary threshold, often relying on intelligence sources that cannot be disclosed in open court. Second, like the CFAA, the EEA is purely reactive: prosecution occurs only after theft has occurred, leaving national security exposed in the interim. In national defense contexts, reliance on ex post prosecutions proves insufficient because the damage from exfiltrated information cannot be undone by subsequent conviction.

Most importantly for this paper's argument, the EEA, like the CFAA, lacks any preventative mechanism. The statute does not mandate that contractors implement insider risk programs, vet subcontractor personnel, or disclose offshore development arrangements as conditions of government contracting. It punishes individual bad actors but places no burden

[33]18 U.S.C. § 1831(a) (2018).

[34]United States v. Aleynikov, 676 F.3d 71 (2d Cir. 2012).

on the organizations whose structural vulnerabilities enable those bad actors to operate. A contractor could employ foreign nationals subject to mandatory intelligence cooperation laws, operate opaque supply chains with minimal visibility into developer identity, and maintain no meaningful insider threat program, yet face no EEA liability until an individual employee steals trade secrets. This ex-post orientation renders the EEA inadequate for addressing structural insider risk.

C. The Espionage Act

The Espionage Act of 1917, codified at 18 U.S.C. §§ 793-798,[35] remains the foundational criminal statute for addressing leaks of classified national defense information. Section 793 criminalizes unauthorized retention or disclosure of national defense information, while Section 798 specifically addresses communications intelligence. The Act has been applied in cases ranging from classic Cold War espionage to modern digital leaks, and its strength lies in its focus on protecting national defense information regardless of the actor's motivation.

Critically for this paper's analysis, Section 793(f) contains a gross negligence provision that differs from the intent requirements of other insider threat statutes. The provision states: "Whoever, being entrusted with ... any document ... relating to the national defense ... through gross negligence permits the same to be removed from its proper place of custody ... shall be fined under this title or imprisoned not more than ten years, or both."[36] This language is notable because it does not require proof of intent to harm the United States

[35] 18 U.S.C. §§ 793, 798 (2018).

[36] 18 U.S.C. § 793(f) (2018) ("Whoever, being entrusted with ... any document ... relating to the national defense ... through gross negligence permits the same to be removed from its proper place of custody ... shall be fined under this title or imprisoned not more than ten years, or both.").

or assist a foreign power. Instead, it penalizes negligent safeguarding when the consequence is loss, theft, or removal of national defense information.

In *Gorin v. United States*,[37] courts established that "national defense information" must be closely held by the government and that its disclosure could potentially damage national security. Applied to modern insider risk scenarios, Section 793(f) could theoretically create liability for gross negligence in digital safeguarding, including failure to vet subcontractors, failure to restrict offshore development of sensitive systems, or failure to implement adequate identity governance. If courts or Congress were to confirm that § 793(f) applies to such negligent digital safeguarding, it could create liability for contractors who permit structural vulnerabilities to persist, a statutory incentive to adopt more rigorous insider risk practices, and the first meaningful mechanism for imposing prospective obligations on contractors rather than merely punishing individual actors after the fact.

Military courts have confirmed that Section 793(f) applies to gross negligence in handling classified materials. In United States v. Roller, the Court of Appeals for the Armed Forces upheld the conviction of a Marine Corps intelligence specialist under 18 U.S.C. § 793(f) for inadvertently removing classified materials from a SCIF and storing them at his residence. The court emphasized that "[t]he purpose of the federal espionage statute is to protect classified documents from any unauthorized procedures such as 'removal from its proper place of custody,'" and that no intent to harm the United States was required for conviction. Sergeant Roller's conduct, which the Navy-Marine Corps Court of Military Review characterized as "his own gross negligence," resulted in a two-year sentence despite

[37]Gorin v. United States, 312 U.S. 19 (1941).

the absence of any evidence that he intended to distribute classified information to unauthorized personnel.[38]

Critically, while Roller and similar military prosecutions have applied Section 793(f) exclusively to individual criminal liability, the statutory text does not limit its reach to natural persons. The provision applies to "whoever, being entrusted with" national defense information who "through gross negligence permits the same to be removed from its proper place of custody." The term "whoever" in federal criminal statutes presumptively includes corporations and other legal entities under 1 U.S.C. § 1, which provides that "the words 'person' and 'whoever' include corporations, companies, associations, firms, partnerships, societies, and joint stock companies, as well as individuals" unless context indicates otherwise. Nothing in Section 793(f) expressly limits its application to natural persons, and the concept of being "entrusted with" national defense information maps naturally onto the relationship between government contractors and the classified or controlled information they handle pursuant to their contracts.

This textual analysis suggests a potentially groundbreaking application of Section 793(f): if a defense contractor is "entrusted with" national defense information through its government contracts, and if that contractor "through gross negligence permits" such information to be "removed from its proper place of custody" by failing to implement adequate insider risk controls, failing to vet subcontractor personnel, or permitting offshore development of sensitive systems without appropriate safeguards, the contractor itself could face criminal liability under the Espionage Act. No court has yet applied Section 793(f) to a

[38] United States v. Roller, 42 M.J. 264 (C.A.A.F. 1995) (affirming conviction under 18 U.S.C. § 793(f) for gross negligence in handling classified materials); United States v. Roller, 37 M.J. 1091, 1096 (N.M.C.M.R. 1993) (characterizing defendant's inadvertent removal of classified materials as "his own gross negligence"). See also United States v. Nishimura, No. 2:15-cr-00114 (E.D. Cal. 2016) (Naval reservist pleaded guilty to unauthorized removal and retention of classified materials under 18 U.S.C. § 793(f) after storing classified information on personal devices in Afghanistan and the United States; sentenced to two years probation despite absence of evidence of intent to distribute).

corporate defendant in this manner, but the statutory language clearly seems to encompass such liability. Were courts or prosecutors to pursue this theory, it would create the first meaningful criminal accountability mechanism for contractors who maintain structural vulnerabilities that enable insider exploitation, transforming Section 793(f) from a tool for punishing individual negligence into a mechanism for imposing prospective duties on organizations handling national defense information.

However, the Espionage Act faces significant limitations. Application to digital environments inside the Defense Industrial Base remains underdeveloped: courts have not directly addressed whether unintentional security flaws or negligent contractor oversight constitute the kind of "gross negligence" that trigger § 793(f) liability. The Act's high evidentiary burden and reliance on prosecuting after disclosure limit its deterrent effect against systemic insider risks. Nonetheless, § 793(f) represents one of the few existing statutory tools that could potentially impose a duty of care on contractors rather than merely criminalizing individual misconduct. This makes its development and application critical to addressing the structural vulnerabilities this paper identifies.

D. Section 889 of the NDAA

Section 889 of the Fiscal Year 2019 National Defense Authorization Act prohibits federal agencies from procuring equipment or services from certain Chinese companies, including Huawei and ZTE, based on national security concerns.[39] It also restricts contractors from using "covered" equipment in performing government contracts. Section 889 reflects Congressional recognition that certain foreign-controlled telecommunications equipment poses unacceptable supply chain risk.

[39]Pub. L. No. 115-232, § 889, 132 Stat. 1917 (2018).

While Section 889 demonstrates that Congress can act to address supply chain security, it is narrowly tailored to equipment and corporate entities. The statute does not directly address employment of foreign nationals in subcontracting roles or vetting of coders embedded in sensitive projects. This gap creates an asymmetry: the Department of Defense may be barred from buying Huawei routers under Section 889 yet is not statutorily barred from contracting with vendors whose developers include PRC nationals subject to mandatory cooperation under China's National Intelligence Law. In other words, Congress has addressed equipment-based threats through statutory prohibition but has left personnel-based threats to regulation (CMMC and DFARS) that relies largely on self-certification, at least for Controlled Unclassified Information and lower classification levels.

Section 889 thus illustrates the piecemeal nature of insider risk regulation. It plugs one hole in the supply chain (equipment vendors) while leaving others (personnel insiders) exposed. A truly comprehensive approach would extend Section 889's logic to personnel, prohibiting contractors from employing foreign adversary nationals in sensitive technical roles, or at minimum requiring disclosure and enhanced vetting. Without such extension, the statutory framework remains incomplete.

E. The Cybersecurity Maturity Model Certification (CMMC)

The Cybersecurity Maturity Model Certification, codified at 32 C.F.R. Part 170,[40] is the Department of Defense's regulatory mechanism for verifying contractor implementation of NIST SP 800-171 security requirements. CMMC aims to standardize cybersecurity practices among contractors, with certification tiers ranging from basic cyber hygiene (Level

[40] 32 C.F.R. § 170.16 (2024) (describing self-assessment and affirmation procedures for Level 1 and Level 2 certification).

1) to advanced practices (Level 3). The framework represents DoD's most significant effort to impose cybersecurity requirements on the Defense Industrial Base.

CMMC's most direct relevance to insider risk lies in its requirement for contractors to implement certain access controls, personnel security measures, and awareness training. The framework incorporates several controls from NIST SP 800-171 that collectively support insider risk mitigation: Security Awareness and Training (AT.L2-3.2.3) requires training personnel to recognize indicators of potential insider threats including social engineering and anomalous behavior; Personnel Security (PS) controls require screening personnel prior to granting access to Controlled Unclassified Information, ongoing monitoring, and managing access upon transfer or termination; Access Control (AC.L2-3.1.5) enforces the principle of least privilege, ensuring users only have access to information necessary for their job functions.

However, CMMC remains disproportionately focused on technical safeguards (access controls, encryption, incident reporting) rather than behavioral or legal mechanisms for managing insider threats. Critically, under 32 C.F.R. § 170.16, contractors at Level 1 and Level 2 may satisfy CMMC requirements through self-assessment and affirmation rather than independent third-party verification. This self-attestation model creates opportunities for contractors to overstate compliance, particularly when government contracts are lucrative and the probability of audit is low.

Specific CMMC requirements illustrate this gap between technical mandates and verification mechanisms. Security requirement SC.L2-3.13.11 ("CUI Encryption") mandates that contractors "[e]mploy FIPS-validated cryptography when used to protect the confidentiality of CUI," requiring cryptographic modules tested and validated under FIPS 140-2 standards for all CUI transmitted or stored outside protected environments. Similarly,

SC.L2-3.13.8 ("Data in Transit") requires contractors to "[i]mplement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission," and SC.L2-3.13.16 ("Data at Rest") requires protection of CUI confidentiality at rest through encryption or physical safeguards. These are substantive technical requirements with real security implications. Yet under 32 C.F.R. § 170.16, contractors seeking "Level 2 (Self)" certification verify compliance with these encryption requirements through self-assessment: the contractor evaluates its own systems, scores its own compliance, uploads the results to SPRS, and has an "Affirming Official" attest to continuing compliance. No independent assessor verifies that FIPS-validated cryptographic modules are actually deployed, that CUI is actually encrypted in transit and at rest, or that the stated security controls exist outside the contractor's own documentation. The regulatory framework thus creates detailed technical requirements but relies on the regulated entity to certify its own compliance, a structural weakness that sophisticated vendors can exploit while maintaining formal compliance.[41]

Legal scholars have long observed that compliance regimes premised on self-certification often devolve into "box-checking" exercises, producing formal compliance without substantive security.[42] As Coglianese and Lazer explain, "direct government supervision is critical when ... the company may not be committed to meeting ... regulatory

[41] See CMMC Assessment Guide – Level 2, Version 2.13, DoD CIO (providing assessment guidance for SC.L2-3.13.11, SC.L2-3.13.8, and SC.L2-3.13.16); 32 C.F.R. § 170.16(a)(1) (2024) (establishing that "[t]he OSA must conduct a Level 2 self-assessment in accordance with NIST SP 800-171A" and upload results to SPRS); 32 C.F.R. § 170.22(a)(1)–(2) (2024) (defining "Affirming Official" as "the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance" and requiring affirmation "attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements"). Third-party C3PAO assessments are required only for contracts specifying "Level 2 (C3PAO)" under 32 C.F.R. § 170.17; many contracts handling CUI require only "Level 2 (Self)" certification.

[42] See Cary Coglianese & David Lazer, Management-Based Regulation: Prescribing Private Management to Achieve Public Goals, 37 LAW & SOC'Y REV. 691, 710-12 (2003).

goals."[43] Companies with strong incentives to win government contracts may calculate that the benefits of understating security deficiencies outweigh the risks of enforcement, particularly when enforcement is reactive rather than proactive. The Microsoft incidents illustrate this dynamic: despite presumably satisfying applicable CMMC requirements, Microsoft operated the digital escorts program for a decade and maintained authentication key management practices that enabled Storm-0558.

This analysis points to CMMC enforcement as one of the two primary mechanisms available to impose meaningful obligations on contractors. Unlike the criminal statutes discussed above, CMMC operates prospectively: it requires contractors to implement security measures before incidents occur, and non-compliance can result in contract ineligibility. But this leverage is only meaningful if DoD enforces CMMC requirements rigorously, conducts meaningful audits of self-attestations, and imposes consequences for non-compliance. Without rigorous enforcement, CMMC risks becoming another compliance exercise that sophisticated vendors can satisfy on paper while maintaining structural vulnerabilities in practice.

F. Synthesis: The Ex-Post Problem

The legal and regulatory frameworks governing insider risk share a fundamental limitation: apart from CMMC enforcement and potential § 793(f) application, they operate almost entirely as ex post mechanisms that punish individual bad actors after harm has occurred. The CFAA and EEA criminalize unauthorized access and trade secret theft but have been judicially narrowed and remain reactive remedies. The Espionage Act addresses leaks of classified defense information but imposes high burdens of proof and, apart from §

[43]Id. at 712 ("In summary, direct government supervision is critical when ... the company may not be committed to meeting ... regulatory goals.").

793(f), requires intent. Section 889 addresses corporate equipment vendors but not personnel-level risks.

None of these statutes impose any affirmative duty on contractors to prevent structural insider risk. A contractor could employ foreign nationals subject to mandatory intelligence cooperation laws, operate completely opaque supply chains, maintain no meaningful insider threat program, and permit offshore development of sensitive systems with no U.S. oversight, yet face no legal liability under the CFAA, EEA, or most Espionage Act provisions until an individual employee commits a crime. The contractor itself bears no responsibility for creating the structural conditions that enable insider exploitation.

This ex-post orientation creates a patchwork ill-suited to the modern threat landscape, where adversarial states exploit contractors, subcontractors, and global supply chains as insider vectors. The only mechanisms that burden contractors prospectively are rigorous CMMC enforcement (which conditions contract eligibility on security compliance) and potential application of § 793(f)'s gross negligence standard (which could create liability for negligent digital safeguarding). These two tools therefore deserve particular emphasis in any reform agenda, as they represent the only existing legal leverage to shift incentives from reactive prosecution to proactive prevention.

V. Gaps in Current Frameworks

A. Overreliance on Self-Attestation

One of the most glaring weaknesses in the current framework is government reliance on contractors to self-attest to compliance with cybersecurity and insider risk standards. Under CMMC 2.0, third-party assessments are required primarily for higher certification tiers (Level 3), leaving Level 1 and Level 2 contractors, who handle the vast majority of

Controlled Unclassified Information, subject only to self-assessment and affirmation. Even when third-party audits occur, they typically verify technical control implementation rather than the behavioral, organizational, and supply chain factors that create structural insider risk.

This reliance creates fertile ground for false confidence in compliance. As illustrated in the Microsoft incidents, even leading technology vendors can overstate readiness with catastrophic consequences when adversarial states exploit vulnerabilities. Self-attestation is particularly problematic in the context of insider risk, where behavioral dynamics, supply chain opacity, and foreign legal obligations cannot be easily quantified through checklists. A contractor could truthfully affirm that it has implemented all 110 NIST SP 800-171 controls while simultaneously operating a digital escorts program that creates direct access pathways for foreign nationals subject to intelligence cooperation laws.

The Coglianese and Lazer analysis of management-based regulation is directly applicable here. Their research identifies categories of regulated entities ranging from those genuinely committed to regulatory goals to those who will cut corners absent direct supervision. When government contracts are lucrative and audit probability is low, companies may rationally calculate that the benefits of understating deficiencies outweigh the risks of enforcement. This dynamic is particularly acute in cybersecurity, where the costs of robust insider risk programs are immediate and visible while the benefits are probabilistic and diffuse. Without mechanisms to verify self-attestations and impose consequences for material misrepresentations, CMMC cannot reliably distinguish between genuine compliance and paper compliance.

B. Subcontractor and Supply Chain Loopholes

Even where prime contractors implement robust security practices, vulnerabilities persist through subcontracting relationships. The digital escorts case exemplifies this pattern:

Microsoft operated the program through arrangements that created direct access pathways for foreign nationals while the Defense Department apparently lacked visibility into the program's existence. Current frameworks fail to close this gap because CMMC requirements flow down to subcontractors imperfectly, prime contractors often lack visibility into subcontractor personnel and practices, there is no statutory requirement to disclose developer nationality or offshore development locations, and foreign subcontractors may face legal obligations under their home country's laws that conflict with U.S. security interests.

The structural deficiencies in federal oversight were confirmed by former federal officials in comments to ProPublica's investigation of Microsoft's digital escorts program. Former Defense Department Chief Information Officer John Sherman characterized the situation as "a case of not asking the perfect question to the vendor, with every conceivable prohibited condition spelled out," adding that a more specific inquiry "would've smoked out this crazy practice." A former official from the General Services Administration, which administers FedRAMP, likened the current cloud assessment process to "a restaurant hiring and paying for its own health inspector rather than the city doing so." These observations highlight fundamental gaps in both CMMC and FedRAMP: the former relies heavily on self-attestation at lower certification levels and imperfect flow down to subcontractors, while the latter depends on third-party assessors hired and paid directly by the companies being assessed, creating inherent conflicts of interest. Microsoft's security documentation distinguished between "screened" and "non-screened" personnel but never specified that "non-screened" personnel included engineers located in mainland China, a disclosure gap that existing frameworks failed to close.[44]

[44] Renee Dudley, Microsoft Didn't Disclose Key Details to U.S. Officials of China-Based Engineers, Record Shows, ProPublica (Aug. 20, 2025), https://www.propublica.org/article/microsoft-china-defense-department-cloud-computing-security (reporting comments from former Defense Department CIO John Sherman and former GSA official regarding structural gaps in FedRAMP oversight process).

This supply chain opacity is particularly dangerous given China's National Intelligence Law. Any Chinese national working on U.S. defense projects, whether as a direct contractor employee, a subcontractor employee, or a cloud service provider administrator, could be subject to compulsory intelligence demands from the Chinese government. Current frameworks do not require contractors to identify such personnel, assess the associated risks, or implement mitigations. The result is that adversarial states can achieve insider access through layered supply chain relationships that remain invisible to both prime contractors and government oversight.

C. Reactive Enforcement Posture

Even the criminal statutes that could theoretically address insider threats suffer from reactive enforcement. The CFAA and EEA require completed offenses before prosecution can occur. The Espionage Act, while broader in scope, still depends on identifying and prosecuting individual actors after disclosure. In the DOJ cases examined below involving PRC-affiliated actors, all defendants were located in China beyond U.S. jurisdiction, rendering extradition unlikely and prosecution largely symbolic. This jurisdictional constraint extends to foreign subcontractors whose activities compromise U.S. systems; even when conduct clearly violates U.S. law, lack of jurisdictional reach undermines enforcement.

The reactive posture creates perverse incentives. Contractors may weigh the low probability of enforcement against the cost of robust insider risk programs, leading to systematic underinvestment in preventative measures. Without statutory penalties for structural vulnerabilities or uniform enforcement mechanisms, insider risk remains an externality borne by the government and taxpayers rather than a liability borne by the vendors who create the vulnerabilities. This dynamic will persist until legal frameworks shift from

punishing individual criminals to requiring contractors to prevent the structural conditions that enable criminal exploitation.

D. Lack of Personnel Transparency Requirements

Current frameworks do not require contractors to disclose basic information about the personnel who access sensitive systems: developer nationality, geographic development locations, subcontractor identities, or affiliations with foreign corporations subject to intelligence cooperation laws. This opacity prevents the government from assessing structural insider risk and prevents contractors from making informed decisions about supply chain security. The digital escorts program persisted for a decade in part because no disclosure requirement forced Microsoft or its subcontractors to reveal that Chinese nationals were writing code for Pentagon systems.

Without personnel transparency, even well-intentioned contractors cannot fully assess their own insider risk exposure. A prime contractor may satisfy every CMMC control, implement state-of-the-art technical safeguards, and conduct regular security training, yet remain unaware that a critical subcontractor employs developers in China who face mandatory intelligence cooperation obligations. The absence of disclosure requirements leaves this vulnerability invisible until exploitation occurs.

VI. Comparative Perspective: Chinese Legal Architecture

A. The National Intelligence Law of 2017

In 2017, the People's Republic of China enacted the National Intelligence Law, imposing sweeping obligations on organizations and individuals to cooperate with state intelligence agencies. Article 7 mandates that "any organization or citizen shall support,

assist, and cooperate with the state intelligence work."[45] This provision effectively transforms every Chinese national and company into a potential instrument of state intelligence, not through voluntary recruitment but through legal compulsion.

From an insider risk perspective, the NIL represents a statutory guarantee of cooperation with the CCP intelligence apparatus. Unlike the United States, where insider risk is treated as a compliance and monitoring issue within organizations, Chinese law ensures that employees and contractors can be compelled to act as insiders when directed by the state. The law also provides secrecy requirements, prohibiting individuals from disclosing that they have cooperated with intelligence agencies. This creates an opaque environment where foreign subcontractors may face irresistible legal obligations to insert backdoors or exfiltrate data without the knowledge of employers or U.S. partners.

Microsoft President Brad Smith's testimony before Congress that Microsoft does not comply with Chinese intelligence requests and that China does not always enforce its laws strains credulity in light of this statutory framework. As Representative Gimenez noted, based on his work on the Select Committee on China, "all companies in China have to cooperate with the intelligence agencies of China and the People's Liberation Army." The NIL creates mandatory cooperation obligations that Chinese nationals and companies cannot legally refuse, regardless of their personal preferences or corporate policies.

The precise legal basis for this compelled secret cooperation deserves elaboration, as it directly creates the structural insider risk this paper addresses. Article 7 of the NIL states: "All organizations and citizens shall support, assist, and cooperate with national intelligence efforts in accordance with the law, and shall protect the secrecy of any national intelligence

[45]National Intelligence Law of the PRC, art. 7 (2017), translated in NPC Observer.

work they are aware of." This provision establishes three distinct obligations: support and assistance, cooperation, and secrecy regarding any intelligence work. The secrecy obligation is particularly significant for insider risk analysis because it means Chinese nationals cannot lawfully disclose their cooperation to foreign employers, including U.S. companies.

Article 14 of the NIL reinforces this compulsory framework, providing that "state intelligence work organs, when carrying out intelligence work, may request relevant organs, organizations, and citizens provide necessary support, assistance, and cooperation." Critically, there is no carve-out for employment relationships with foreign companies, no exception for employees of U.S. defense contractors, and no provision allowing disclosure to employers for compliance or insider-risk reporting purposes. Article 10 further authorizes intelligence agencies to "employ necessary means, tactics, and channels to carry out intelligence work," language interpreted broadly to include covert cooperation and nondisclosure requirements.

The State Security Law of 2015 reinforces these obligations. Article 11 requires that citizens and organizations "keep state secrets" and "provide truthfully any needed support" to state-security authorities. Together, these provisions create an interlocking legal framework that compels Chinese nationals to assist intelligence services while prohibiting disclosure of that assistance. Western intelligence assessments from the FBI, ODNI, and allied agencies have consistently confirmed that Chinese nationals cannot meaningfully resist direct requests from security forces or law enforcement, and that the obligation to maintain secrecy applies regardless of the individual's employment situation or the nationality of their employer.

The insider risk implications of this legal architecture are profound and unavoidable. Under the NIL, a PRC citizen can be compelled to assist Chinese intelligence at any time, they are required to keep that assistance secret under penalty of law, and they cannot lawfully

inform a U.S. employer if the state instructs secrecy. This creates a structural insider-risk vector for any organization employing PRC nationals who remain under PRC jurisdiction or coercive reach. No amount of employee training, background screening, or corporate policy can overcome legal obligations that compel secret cooperation with a foreign intelligence service. The NIL thus transforms the employment of Chinese nationals in sensitive positions from an individual risk assessment into a categorical structural vulnerability.

B. The Data Security Law and Counter-Espionage Law

China's Data Security Law, adopted in 2021, further entrenches state control over information by imposing obligations on organizations to classify and protect data according to its "importance to national security, the national economy, and the public interest." Article 35 requires entities handling "important data" to undergo national security reviews before transferring such data abroad.[46] From an insider risk perspective, the DSL expands the Chinese state's ability to compel companies and individuals to treat data as a national asset. Multinational corporations with R&D centers in China may be forced to provide access to sensitive data under the pretext of classification reviews. In practice, this framework not only facilitates state-directed insider risk but institutionalizes it: employees may be required to act as conduits for data transfer under the guise of legal compliance with Chinese domestic law.

The Counter-Espionage Law, amended in 2023, broadens the definition of espionage and expands state investigative powers.[47] The law authorizes the Ministry of State Security to conduct inspections, seizures, and surveillance to prevent espionage activities. Importantly, it allows the state to compel organizations and individuals to assist counter-espionage efforts,

[46]Data Security Law of the PRC, art. 35 (2021), translated in China Law Translate.

[47]Counter-Espionage Law of the PRC (2023 amendments), analysis in Stanford China Guiding Cases Project.

further reinforcing the compulsory nature of insider cooperation. One troubling aspect is the law's vagueness: espionage is defined so broadly that almost any data activity could fall within scope. For Chinese nationals working on U.S. defense projects, this means they may be compelled not only to exfiltrate information but also to deny cooperation with U.S. counterintelligence efforts under threat of prosecution in China.

The combination of the NIL, DSL, and Counter-Espionage Law creates a layered legal regime that systematically weaponizes insiders for the benefit of the Chinese state. Any Chinese national with access to U.S. defense systems faces overlapping legal obligations to cooperate with state intelligence, protect data as a national asset, and assist counter-espionage efforts, all while maintaining secrecy about such cooperation. U.S. contractors who employ Chinese nationals in any capacity unwittingly import individuals bound by these statutory duties, creating structural insider risk that no amount of individual vetting can fully address.

C. Contrast with U.S. Legal Framework

The U.S. approach to insider risk stands in stark contrast to China's mandatory cooperation laws. American statutes such as the CFAA, EEA, and Espionage Act are primarily punitive and reactive. They criminalize misconduct but do not require proactive loyalty or disclosure. Similarly, frameworks like CMMC impose compliance requirements but do not create statutory duties for individuals to act in the interest of national security. This asymmetry places the United States at strategic disadvantage: China can compel its citizens abroad to act as insiders, while the United States must rely on voluntary loyalty and organizational safeguards.

Furthermore, U.S. contractors who employ Chinese nationals may unwittingly import individuals bound by statutory duties to act on behalf of the CCP. Current American laws, Section 889 included, do not address this personnel-level risk. The structural implication is

clear: any Chinese subcontractor, coder, or vendor employee with access to U.S. defense systems is a potential insider threat not merely by personal choice but by legal compulsion. In this context, U.S. reliance on self-attestation, patchwork enforcement, and vendor goodwill is profoundly inadequate.

VII. Proposed Legal and Policy Reforms

The following reforms are organized by implementing authority and prioritized by criticality. Congressional reforms require new legislation. Executive branch reforms can be implemented through regulatory action under existing authority, with national security regulations exempt from APA notice-and-comment requirements under 5 U.S.C. § 553(a)(1).[48] The organizing principle throughout is shifting from ex post punishment of individual actors to prospective requirements that burden contractors to prevent structural vulnerabilities.

A. Congressional Action: Statutory Reforms

1. CRITICAL: Clarify 18 U.S.C. § 793(f) Application to Digital Safeguarding. Congress should amend § 793(f) or enact clarifying legislation confirming that gross negligence in safeguarding digital national defense information, including failure to vet subcontractors handling sensitive systems, failure to restrict offshore development, and failure to implement adequate identity governance, may constitute a violation. Proposed language might specify that "gross negligence" includes permitting access to national defense information systems by foreign nationals subject to mandatory intelligence cooperation laws of adversarial nations without adequate mitigation measures, failing to disclose offshore

[48] 5 U.S.C. § 553(a)(1) (2018).

development of national defense systems to contracting agencies, and operating supply chains with material opacity regarding personnel identity and location. This reform would transform § 793(f) from an underutilized provision into a meaningful tool for imposing prospective duties on contractors.

2. CRITICAL: Amend Computer Fraud and Abuse Act. Congress should amend the CFAA to cover misuse of authorized access with intent of harming national security, restoring the tools narrowed by *Van Buren* while maintaining appropriate limits against over criminalizing ordinary employee activity. Proposed language might add to 18 U.S.C. § 1030(e) that "authorized access" shall exclude access motivated by external coercion, undeclared foreign affiliations, or intent to benefit foreign governments, regardless of the formal authorization status of the user's account.

3. HIGH PRIORITY: Expand Section 889 Logic to Personnel. Congress should enact legislation in the future NDAA prohibiting employment of foreign adversary nationals in sensitive technical roles on defense contracts, paralleling Section 889's prohibition on covered equipment. This would extend the supply chain security logic Congress applied to telecommunications equipment to the personnel dimension, recognizing that individuals subject to mandatory intelligence cooperation laws pose risks comparable to equipment from adversary-controlled companies.

4. HIGH PRIORITY: Mandatory Insider Incident Reporting. Congress should require standardized reporting of insider incidents within 72 hours, create a centralized database for tracking incidents across the Defense Industrial Base (with protection from FOIA disclosure to preserve contractor confidentiality), and enable systemic risk analysis. This requirement could be incorporated into CMMC as a condition for Level 2 and above certification.

B. Executive Branch Action: Regulatory Reforms

1. CRITICAL: Strengthen CMMC Insider Threat Requirements and Enforcement. The Department of Defense should modify CMMC to require behavioral risk monitoring beyond basic awareness training, enhanced personnel vetting including disclosure of foreign national status and affiliations, whistleblower protections for insider threat reporting, independent audits of self-attestations with meaningful consequences for material misrepresentations, and designated insider threat program managers per NISPOM requirements.[49] Most critically, DoD must commit to rigorous enforcement of existing and enhanced CMMC requirements. Without enforcement, CMMC remains a compliance exercise that sophisticated vendors can satisfy on paper while maintaining structural vulnerabilities. Enforcement should include random audits of self-attestations, investigation of reported incidents, and meaningful consequences including contract termination and debarment for material non-compliance.

2. CRITICAL: Personnel Transparency Requirements. Executive agencies with FAR authority[50] should require disclosure of developer nationality, subcontractor personnel identity, geographic development locations, and developer affiliation with foreign corporations subject to intelligence cooperation laws. This requirement would create visibility into supply chain personnel and enable assessment of foreign legal coercion risk.

3. RECOMMENDED: Offshore Development Restrictions. DoD should adopt restrictions on controlled technical work performed in high-risk jurisdictions, by companies under foreign intelligence obligations, and in offshore facilities in adversarial nations. At minimum, contractors should be required to disclose offshore development and obtain agency

[49]DoD 5220.22-M, NISPOM, § 1-202.

[50]48 C.F.R. § 1.103 (2024).

approval before permitting foreign nationals in adversary countries to access systems containing Controlled Unclassified Information.

4. RECOMMENDED: Vendor Accountability Framework. Create negligence-based liability with safe harbor for CMMC-compliant vendors who demonstrate good faith compliance. As Coglianese and Lazer observe, increasing the costs of failing to meet regulatory goals changes company calculations and incentivize genuine compliance. This framework would balance accountability with appropriate incentives, ensuring that contractors who invest in robust insider risk programs receive meaningful legal protection while those who cut corners face consequences.

VIII. Conclusion

Insider risk is neither novel nor abstract. From Cold War double agents to twenty-first-century contractor coders, insiders have always represented the hardest threats to detect and most dangerous to ignore. What has changed is scale and complexity in the digital age. Today, malicious insiders need not physically smuggle documents; they can exfiltrate terabytes with keystrokes. Moreover, globalized supply chains mean insiders are no longer limited to U.S. employees but may include foreign nationals legally compelled by adversarial governments to serve as intelligence assets.

The case studies examined underscore these dynamics. Microsoft's digital escorts program highlights how structural vulnerabilities can persist for years within nominally compliant contractors, creating direct access pathways for foreign nationals subject to mandatory intelligence cooperation laws. The Storm-0558 intrusion reveals dangers of concentration risk and lack of accountability when trusted providers fail to maintain basic security hygiene. Together, these cases demonstrate that the United States faces insider risk

not as isolated failures but as structural vulnerabilities embedded in how the Defense Industrial Base operates.

Current legal frameworks, while important, are overwhelmingly reactive and incomplete. The CFAA and EEA criminalize unauthorized access and trade secret theft but provide little preventative effect: they punish individual bad actors after harm has occurred but impose no burden on contractors to prevent the structural conditions enabling exploitation. The Espionage Act applies to leaks of national defense information but imposes high evidentiary burdens. Section 889 restricts procurement from adversarial corporations but ignores personnel-level threats. CMMC, though promising, risks becoming a technical compliance exercise with limited attention to behavioral realities of insider exploitation.

The central argument of this paper bears emphasis: existing legal frameworks punish individual criminals but do not burden contractors. A contractor could employ foreign nationals subject to mandatory intelligence cooperation laws, maintain completely opaque supply chains, operate offshore development with no U.S. oversight, and implement no meaningful insider threat program, yet face no legal liability until an individual employee commits a crime. The contractor itself escapes responsibility for creating the structural conditions that enable insider exploitation.

Only two mechanisms in the current framework impose prospective obligations on contractors: rigorous CMMC enforcement and potential application of 18 U.S.C. § 793(f)'s gross negligence standard. CMMC conditions contract eligibility on security compliance, but only if DoD enforces requirements rigorously rather than accepting self-attestations at face value. Section 793(f) could create liability for grossly negligent digital safeguarding, but only if courts or Congress confirm its application to the structural vulnerabilities discussed in this paper. These two tools therefore deserve particular emphasis in any reform agenda, as they

represent the only existing legal leverage to shift contractor incentives from reactive posture to proactive prevention.

By contrast, China's legal architecture demonstrates the stakes of this asymmetry. Under the National Intelligence Law, Data Security Law, and Counter-Espionage Law, every Chinese national and corporation is legally obligated to cooperate with state intelligence and to conceal that cooperation. For the United States, this means every Chinese subcontractor, coder, or vendor employee with access to defense systems is a potential insider threat not merely by personal choice but by legal compulsion. In this context, U.S. reliance on self-attestation, patchwork enforcement, and vendor goodwill is profoundly inadequate.

The reforms proposed offer a path forward. Clarifying § 793(f)'s application to digital safeguarding would create statutory incentive for contractors to address structural vulnerabilities. Strengthening CMMC with rigorous enforcement, personnel transparency requirements, and expanded authority would institutionalize preventative measures across the Defense Industrial Base. Extending Section 889's logic to personnel would close the gap Congress left when it addressed equipment-based threats but not personnel-based threats. Vendor liability frameworks would realign incentives by ensuring negligent providers bear responsibility for security failures rather than externalizing costs to the government.

No legal regime can fully eliminate insider risk. The nature of trust relationships in organizational and national security contexts ensures vulnerabilities will always exist. But law can and must evolve to reduce those vulnerabilities, mitigate systemic risks, and shift incentives toward proactive security. In an era where adversarial states weaponize insiders through legal compulsion, the United States cannot afford a fragmented and reactive posture that punishes individual criminals while leaving contractors free to create the structural conditions enabling exploitation.

The stakes are not merely contractual disputes or compliance failures; they are protection of classified systems, critical infrastructure, and the integrity of democratic government. Insider risk is not just a technical issue but a constitutional one, implicating Congress's duty to provide for the common defense and the executive's obligation to protect national security. If the United States fails to reform its insider risk framework, if it continues to rely on ex post prosecution of individual criminals rather than prospective requirements on contractors, it risks allowing adversaries to achieve through insiders what they cannot accomplish through open confrontation. The reforms proposed here provide a roadmap for that response: organized by implementing authority, prioritized by criticality, and grounded in the recognition that only mechanisms which burden contractors can meaningfully address structural insider risk.