

The Supreme Art of War, on Subduing the Enemy without Fighting^{*}: Defending Defense Supply Chain Against Foreign Adversaries by Taking Proactive Measures to Enforce §889(a)(1)(B) of the Fiscal Year 2019 National Defense Authorization Act

MAJOR JUNGMOO LEE[†]

TABLE OF CONTENTS

I. “ALL WARFARE IS BASED ON DECEPTION”	1
II. “ <i>PREVENTING THE JUNCTION OF ENEMY FORCES</i> ”: ENACTMENT OF SECTION 889 FISCAL YEAR 2019 NDAA AND ITS ENFORCEMENT MECHANISM.....	3
A. <i>What is Section 889 of Fiscal Year 2019 NDAA?</i>	3
III. “ <i>RAPIDITY IS THE ESSENCE OF THE WAR</i> ”: THE CRITICAL NEED FOR A MULTI-DOMAIN APPROACH TO ENFORCING SECTION 889.....	7
A. <i>Domestic and International Risks posed by the PRC Cyber Operations and their Impact on U.S. National Security</i>	7

^{*} Sun Tzu, *The Art of War*, in THE COMPLETE ART OF WAR 22 (Lionel Giles trans., Start Publishing LLC, 2012).

[†] Judge Advocate, United States Air Force. LL.M., 2022, The Judge Advocate General’s Legal Center and School, United States Army, Charlottesville, Virginia; J.D., 2015, Emory University, School of Law, Atlanta, Georgia; B.A., 2010, University of Illinois, Urbana-Champaign. Member of the Bar of Georgia. The views presented are those of the author and do not necessarily represent the views of DoD or its components. The Author would like to thank her advisors, Lieutenant Colonel Craig M. Scroggins, United States Army, and Major Nicole A. Vele, United States Air Force. The author would like to further thank Mr. Kurt H. Eberle, Major Timothy P. Oster, United States Air Force, and Major Tyler C. Weeks, United States Air Force, for their guidance and input.

1. Threats and Responses against the U.S. Defense Supply Chain and Critical Infrastructure	7
2. Disjointed Response to Cyber Threats: How the Race to 5G is Fracturing the Bond Among the U.S. and its Coalition Partners	9
B. <i>The Inadequacy of the FCA in Enforcing Section 889 Violations</i> ...	12
IV. “[COUNTER] THE ENEMY’S POWER; FORCE HIM TO REVEAL HIMSELF”: SOLUTIONS TO ENHANCE FCA LITIGATION AND TO ENCOURAGE CONTRACTOR PARTICIPATION IN SECTION 889....	15
A. <i>Increasing the Amount of Information to be Provided in the Contractor Certification Process</i>	16
B. <i>Requiring a Third-Party Audit for Contractors with a Higher Risk of Violating Section 889</i>	20
1. The Need for a Third-Party Audit in Section 889 Implementation and Enforcement	20
2. Requiring a Third-party Audit for Overseas Prime Contractors and Certain Domestic Prime Contractors	22
C. <i>Encouraging the Contractors to Utilize the Third-Party Auditors Through FAR-based Incentives</i>	24
V. IN CONCLUSION: “HE WHO CAN MODIFY HIS TACTICS IN RELATION TO HIS OPPONENT AND THEREBY SUCCEED IN WINNING, MAY BE CALLED A HEAVEN-BORN CAPTAIN.”.....	25
Appendix A	1
Appendix B	2

In my discussions. . . with President Xi, I told him, “We welcome the competition. We’re not looking for conflict.” But I made absolutely clear that we will defend America’s interests across the board. America will stand up to unfair trade practices that undercut American workers and American industries, like subsidies from state—to state-owned operations and enterprises and the theft of American technology and intellectual property.¹

I. “ALL WARFARE IS BASED ON DECEPTION”²

On 19 July 2021, the Secretary of State, Mr. Antony J. Blinkin, along with other nations, publicly condemned the People’s Republic of China (PRC) for engaging in cyber espionage by hacking Microsoft Exchange servers.³ This latest set of hacking was accomplished by a group of Chinese government-sponsored hackers known as “Hafnium,” who target infectious disease researchers, law firms, higher education institutions, defense contractors, policy think tanks, and nongovernmental organizations to extract information.⁴ The estimated impact of this brazen move included over 60,000 known victims globally, which included many small and medium-sized businesses.⁵ This is not the first time the PRC has managed to successfully breach the private sector cyber defense line. According to the Joint Cybersecurity Advisory, between 2011 and 2013, the PRC was able to infiltrate the cyber defense line of 23 U.S. pipelines.⁶ It was opined that the attack was conducted “for the purpose of holding U.S. pipeline infrastructure at risk” and to further develop Chinese cyberattack capabilities to physically damage or disrupt the pipelines.⁷ Alarming, according to a statistical analysis by Forbes from 2014, the PRC dominated 43% of the world’s internet attack traffic,⁸ highlighting the ever-increasing threat to our private and public cyber domains.

Though written a thousand of years ago, Sun Tzu’s words ring true: warfare is won through deception.⁹ Failing to outmaneuver the PRC in the game of deception will lead to the defeat of the U.S. industrial base and will have catastrophic consequences. In response to the

¹ Joseph Biden, Jr., President of the United States, Address to Joint Session of Congress (Apr. 28, 2021), <https://millercenter.org/the-presidency/presidential-speeches/april-28-2021-address-joint-session-congress>;

² Sun Tzu, *The Art of War*, in *THE COMPLETE ART OF WAR* 16 (Lionel Giles trans., Start Publishing LLC, 2012).

³ Press release, U.S. Dep’t of State, Responding to the PRC’s Destabilizing and Irresponsible Behavior in Cyberspace (July 19, 2021), <https://www.state.gov/responding-to-the-prcs-destabilizing-and-irresponsible-behavior-in-cyberspace/>.

⁴ Tom Burt, *New Nation-State Cyberattacks*, MICROSOFT: ON THE ISSUES (Mar. 2, 2021), <https://blogs.microsoft.com/on-the-issues/2021/03/02/new-nation-state-cyberattacks/>.

⁵ William Turton & Jordan Robertson, *Microsoft Attack Blamed on China Morphs Into Global Crisis*, BLOOMBERG (Mar. 6, 2021), <https://www.bloomberg.com/news/articles/2021-03-07/hackers-breach-thousands-of-microsoft-customers-around-the-world>.

⁶ Cybersecurity & Infrastructure Security Agency, Joint Cybersecurity Advisory, Chinese Gas Pipeline Intrusion Campaign, 2011 to 2013 (2021).

⁷ *Id.*

⁸ Niall McCarthy, *China Is The World’s Top Source Of Internet Attack Traffic*, STATISTA (Oct. 8, 2014), <https://www.statista.com/chart/2801/china-is-the-worlds-top-source-of-internet-attack-traffic/>.

⁹ Sun Tzu, *supra* note 2.

increased cyber and espionage attempts by the PRC, the U.S. enacted Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (FY 2019 NDAA).¹⁰ Section 889 operates in two parts; the first part prevents all federal agencies from purchasing telecommunication and video surveillance equipment or services manufactured or provided by five named companies originating from the PRC.¹¹ The second part, which has raised significant public concerns,¹² targets those who wish to contract with the U.S. government by preventing the government from entering into a contract with any contractors who “use(s) any equipment, system, or service that uses prohibited telecom as a substantial or essential component of any system, or as critical technology as part of any system.”¹³ According to some industry critics, however, the lack of clarity in the statute’s scope and its applicability has stifled the federal contracting process.¹⁴

So, will Section 889, despite the criticism it faces, successfully stop the cyber threats from our adversaries once it is time for full implementation?¹⁵ If it does not, what can be done to improve its enforcement mechanism while balancing out the competition interest of the federal acquisition system? This paper proposes that the current model of relying on self-certification of the individual contractor and the False Claims Act (FCA)¹⁶ to enforce §889(a)(1)(B) is inadequate in preventing cyber threats that Section 889 was meant to protect against. Instead, rather than focusing on enforcement, the government must pivot to educating and motivating the contractor base to encourage greater compliance. To fully expand upon this principle, Part I of this paper will discuss the background of Section 889 and the current certification and enforcement procedures for §889(a)(1)(B). Part II will analyze why the current enforcement falls short of achieving the purpose of the statute, and why there is a need to establish a tougher standard to create a greater safeguard against cyber espionage in the government supply chain system. Part III proposes three potential solutions to fortify Section 889 compliances and discusses the pros and cons of each proposal.

¹⁰ John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, § 889, 132 Stat. 1636 (2018) [hereinafter FY19 NDAA].

¹¹ The ban also applies to Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities). *Id.* § 889(f)(3)(B).

¹² See e.g., Roger Waldron, *Section 889 Implementation: Language Changes That May Have Big Consequences*, FEDERAL NEWS NETWORK (Aug. 14, 2020), <https://federalnewsnetwork.com/commentary/2020/08/section-889-implementation-language-changes-that-may-have-big-consequences/>; *SIA’s Comments on NDAA Section 889 Part B Implementing Rules*, SEC. INDUS. ASSOC., <https://www.securityindustry.org/report/sias-comments-on-ndaa-section-889-part-b-implementing-rules/> (last visited Mar. 28, 2022); *The Section 889B Prohibition. . . Legislative Mess Begets Regulatory Mess?*, DENTONS (Sept. 29, 2020), <https://www.dentons.com/en/insights/articles/2020/september/29/the-section-889b-prohibition-a-handful-of-regulatory-messiness>.

¹³ FY19 NDAA.

¹⁴ E.g., letter from National Defense Industry Association to General Services Administration (Mar. 12, 2021) (listing various questions collected from the industry regarding implementation, stating that “[t]he full extent of the impact that Sec. 889(a)(1)(B) will have on subcontractors is currently unknown but we assume that the prohibition will be interpreted to preclude prime contractors from doing business with subcontractors that use Huawei/ZTE equipment”).

¹⁵ The Department of Defense (DoD) has received a waiver until 30 September 2022 for full implementation. Memorandum from John Ratcliffe, Dir. of Nat’l Intel., to Ellen M. Lord, Under Sec’y for Acquisition and Sustainment, Dep’t of Def. (Sept. 29, 2020).

¹⁶ False Claims Act (FCA), 31 U.S.C. §§ 3729–3733.

II. “PREVENTING THE JUNCTION OF ENEMY FORCES”¹⁷: ENACTMENT OF SECTION 889 FISCAL YEAR 2019 NDAA AND ITS ENFORCEMENT MECHANISM

To understand why Section 889 in its current format is inadequate to address the cybersecurity needs of the U.S. defense supply chain system, we must first understand what Section 889 is and how it is enforced. This section intends to achieve that goal by discussing the background of Section 889 of the FY 2019 NDAA. It will then look at how Section 889, specifically, part B, is implemented through the Federal Acquisition Regulation (FAR) and the reaction from the private sector regarding its implementation. It will then discuss the current certification method and the enforcement of that certification through the traditional FAR methods, and more importantly, through the Foreign Claims Act (FCA).

A. What is Section 889 of Fiscal Year 2019 NDAA?

Section 889 of FY 2019 NDAA was enacted as a response to the acts of Chinese cyber espionage against U.S. private and public sector interests, including critical infrastructure and the defense supply chain system.¹⁸ Namely, the law prevents certain Chinese companies such as Huawei Technologies (Huawei) from supplying telecommunication equipment and services to the U.S. government.¹⁹ Section 889 is mainly a two-part prohibition.²⁰ The first section, §889(a)(1)(A), limits the Government’s ability to procure any equipment, system, or service that is substantially or essentially supported by telecommunications equipment or services that fall under the definition of covered telecommunication. Covered telecommunications equipment and services (“CTES”) is defined at §889(d)(3), which includes, among others, telecommunication equipment and

¹⁷ Sun Tzu, *supra* note 2, at 24.

¹⁸ See “we need to start baking security requirements into the design of our systems. Start with our weapons platforms and systems, and then we have got to start looking at critical infrastructure. To me, that is partially a Federal acquisition reform issue.” *Cyber Threats from China, Russia, and Iran: Protecting American Critical Infrastructure: Hearing Before Subcommittee on Cybersec., Infrastruc. Prot., and Sec. Tech. of the Comm. on Homeland Sec. H. of Rep.*, 113th Cong. 41 (2012) (statement of Director of Homeland Security Policy Institute, George Washington University, Mr. Frank Cilluffo); MIKE ROGERS & C.A. RUPPERSBERGER, PERMANENT SELECT COMM. ON INTEL., INVESTIGATIVE REPORT ON THE U.S. NATIONAL SECURITY ISSUES POSED BY CHINESE TELECOMMUNICATIONS COMPANIES HUAWEI AND ZTE (2012); Daniel R. Coats, Director of National intelligence, Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community, 5 (Jan. 29, 2019). Initially, it seems the focus on cyber threats from the PRC arose out of intellectual theft via exportation of U.S. technologies and media contents rather than importation of Chinese technologies. See *U.S.-China Current Trade and Investment Policies and their Impact on the U.S. Economy: Hearing Before U.S.-China Sec. R. Comm.*, 580 (2001); see also MARTHA BAYLES, WHO WILL RULE THE WEB? HUAWEI, HOLLYWOOD, AND THE BATTLE FOR 5G, THE AMERICAN INTEREST (May 29, 2019). The concern also evolved into the PRC’s expansion to African nations, providing telecommunication equipment and products. See *Information Controls, Global Media Influence, and Cyber Warfare Strategy: Hearing before the U.S.-China Econ. and Sec. R. Comm.*, 115th Cong. 163 (2017).

¹⁹ See Hearing on National Defense Authorization Act for Fiscal Year 2019 and Oversight of Previously Authorized Programs Before the Comm. on Armed Serv. H. of Rep., 115th Cong. 55–57 (2018) (statement of Mike Gallagher, Member, H. Comm. on Armed S.).

²⁰ FY19 NDAA, § 889. The entirety of the relevant section of the statute can be found in App. A.

video surveillance services produced by Huawei and ZTE corporation, their subsidiaries, and affiliates (“Covered Entities”).²¹ The statute also covers any unnamed organization that is later deemed to be connected or controlled by the PRC.²² The second portion of the statute, §889(a)(1)(B) (“Section 889 Part B”), which has garnered much controversy,²³ prevents those who seek to contract with the U.S. government from using a CTES. Specifically, this portion of Section 889 prohibits the government from contracting with contractors who use a CTES as “a substantial or essential component of any system, or as critical technology as part of any system.”²⁴ This ban on CTES includes all systems used by the contractor, regardless of whether it was being used to meet the government’s requirement.²⁵

Despite what seems to be a relatively straightforward statute, the response from the public regarding Section 889 Part B shows that without further guidance and clarification, the statute’s broad language could lead to an unprecedented impact on the federal acquisition system. Section 889 is implemented for government agencies and contractors through FAR Subpart 4.21. As with any other regulations, the implementation of Section 889 through the FAR involved federal rulemaking procedures, such as notice and comment period.²⁶ The comments from the industry submitted during the rulemaking process of Section 889 Part B implantation provides a great purview of the complexity of applying this statute. In July and August of 2020, two interim rules addressing Section 889 Part B’s contractor certification process were released.²⁷ In a comment, the Rural Wireless Association estimated that at least 25% of small rural carriers will become overwhelmed by the cost of compliance without a

²¹ The definition also includes video surveillance and telecommunication equipment used for national security purposes that are produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company, as well as their subsidiaries and affiliates. *Id.* § 889. The entirety of the relevant section of the statute can be found in App. B.

²² The inclusion will require determination by the Secretary of Defense in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation. *Id.* § 889(f)(2).

²³ *Infra* note 92 and accompanying text.

²⁴ FY19 NDAA, § 889(a)(1)(B).

²⁵ *Id.* The statute does provide certain explicit exemptions; namely, under § 889(b)(3), and waivers, under § 889(d). Entities and agencies may request individual exemptions for case-specific procurement per § 889(d)(1) and (2). However, the entity must provide a compelling justification, and within thirty days of approval, the head of the agency must provide a thorough report regarding the covered equipment and a phase-out plan to congressional committees. The Director of National Intelligence, per § 889(d)(2), may also grant an extension beyond the implementation date of the statute if the director determines the waiver is in the national security interest.

²⁶ For a primer on agency rulemaking and authority to issue regulations, review OFF. OF THE FED. REG., A GUIDE TO THE RULEMAKING PROCESS (2011), https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

²⁷ Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, 84 Fed. Reg. 135, 42,665–42,679 (July 14, 2020) (to be codified at 48 C.F.R. pt. 13, 39, and 52) [hereinafter July Interim Rule]; Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment, 84 Fed. Reg. 167, 53,126–53,134 (Aug. 27, 2020) (to be codified at 48 C.F.R. pt. 1, 4, 12, 13, 39, and 52) [hereinafter August Interim Rule] The July rule created two FAR Subsections that addressed the level of inquiry required for a contractor to certify that they are not using covered telecommunication equipment or service and report the use of prohibited equipment or services discovered during the performance of a contract. *See* FAR 52.204-24 (2021). The August rule refined the July rule by adding that the certification process can be made on annual basis rather than offer-by-offer. FAR 52.204-25 (2021).

more narrowly tailored proposed Section 889 Part B.²⁸ Likewise, the Internet Association submitted comment stating that without further tailoring the definition of CTES to only apply to substantial or essential component per the statutory language, the industry will be faced with “unreasonably time-consuming, especially considering how all-encompassing it will have to be; unpredictably expensive, especially because of the breadth of no-risk or low-risk components involved in the operations of contractors of any size.”²⁹ Though it is expected that a final rule regarding Section 889 Part B will be released in a near date,³⁰ no such rule has been in place as of August 2022.

B. Enforcing Section 889 Through the False Claims Act

As stated above, Section 889 Part B requires prime contractors must first certify whether they are utilizing a CTES before entering a contract with the Government. Understanding how this certification is satisfied is the key to weighing whether Section 889 is an effective tool against Chinese operations, as the certification serves as the basis for enforcing Section 889 violation through the False Claims Act (FCA).³¹ This section provides a cursory look into what the FCA is and how it is utilized.

A prime contractor may satisfy Section 889 Part B by self-certifying³² that they do not use covered equipment or services so long as there has been a “reasonable inquiry” conducted by the entity.³³ Reasonable inquiry is defined in the FAR as “an inquiry designed to uncover any information in the entity’s possession about the identity of the producer or provider of CTES used by the entity.”³⁴ The interim rules do not give a substantive explanation of what that inquiry should look like, other than stating that it need not include an internal or a third-party audit.³⁵ This certification is required only from the prime

²⁸ Rural Wireless Association, Inc, Comment Letter on Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment; (FAR Case 2019-009) (Dec. 7, 2018), <https://www.fcc.gov/ecfs/document/12080817518045/1>.

²⁹ Internet Association, Comment Letter on Prohibition on Contracting With Entities Using Certain Telecommunications and Video Surveillance Services or Equipment; (FAR Case 2019-009) (Oct. 26, 2020), <https://www.regulations.gov/comment/FAR-2020-0051-0029>. The FAR council is not deaf to these concerns. In its July rule, the FAR council noted that “this rule is one of a series of actions with regard to section 889 and the impact and costs to all industry sectors . . . is not well understood and is still being assessed. July Interim rule, 42,668.

³⁰ Fed. Acq. Reg., Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment (FAR Case 2019-009), REGULATIONS.GOV, <https://www.regulations.gov/docket/FAR-2019-0009/unified-agenda> (displaying target date of Aug 2021 as final rule date). There has been a partial final rule regarding § 889(a)(1)(A) by the DoD. Defense Federal Acquisition Regulation Supplement: Covered Defense Telecommunications Equipment or Services (DFARS Case 2018–D022), 86 Fed. Reg. 10, 3,832–3,835 (Jan. 15, 2021) (to be codified at 48 C.F.R. pt. 204, 212, 213, and 252) (adopting the interim rules for the DoD as initially published in 84 Fed. Reg. 72231 as a final rule regarding § 889(a)(1)(A) for the DoD).

³¹ 31 U.S.C. §§ 3729–3733.

³² See FAR 52.204-24 (2021); FAR 52.204-25 (2021); FAR 52.204-26 (2020).

³³ “Reasonable inquiry means an inquiry designed to uncover any information in the entity’s possession about the identity of the producer or provider of covered telecommunications equipment or services used by the entity that excludes the need to include an internal or third-party audit.” FAR 52.204-25 (2021).

³⁴ *Id.*

³⁵ *Id.*

contractor and excludes subcontractors from having to make any independent representation to the Government.³⁶

Should a contractor misrepresent their certification, that contractor may be held liable for a civil and criminal penalty under the FCA.³⁷ Since its enactment in 1863 during the American Civil War, the FCA has been used to prevent contractors from defrauding the U.S. government.³⁸ Under the FCA, those who make a false claim,³⁹ that is, make a knowing presentation of false record, material statement, and/or claim of payments, are in breach of the law.⁴⁰ Knowingly means the actor has actual knowledge of the information, acts in deliberate ignorance of the truth, or acts in reckless disregard of the truth.⁴¹ A claim under the FCA can be brought by the Government as well as by private persons.⁴² Actions brought on by private persons, also known as relators, are called *qui tam* suits,⁴³ under which the successful litigant may keep for themselves a portion of the recovered damages.⁴⁴ The penalties of an FCA violation per claim are between \$11,665 and \$23,331⁴⁵ and can reach a hefty amount as the government may also seek treble damages, as well as the cost of the civil action, to recover said damages.⁴⁶ However, despite these enforcement procedures and their potential penalties, a pivotal question remains: Are these measures enough to deter future

³⁶ July Interim Rule, 42,666. The certification is made electronically through System for Award Management's (SAM) entity registration information, where the certification will be submitted annually rather than by case-by-case basis. See *id.* 42666; GEN. SERV. ADMIN., SAM RELEASE NOTES BUILD 2020-10-24, at 3 (Oct. 24, 2020). However, a contractor would still be required to submit an "offer-by-offer" representation if they had represented that they do use the covered telecommunication equipment or service. See July Interim Rule, 42666; GEN. SERV. ADMIN., SAM RELEASE NOTES BUILD 2020-10-24, at 3 (Oct. 24, 2020).

³⁷ Another option to address to breach is through the FAR. Under the FAR, a failure to submit an accurate representation can be the basis of termination for default. "As a strictly contractual matter, an organization's failure to submit an accurate representation to the Government constitutes a breach of contract that can lead to cancellation, termination, and financial consequences." August Interim Rule, 53,129. (discussing the regulatory impact of § 889(a)(1)(B)). This would entitle the government to any liquidated damages in addition to any excess repurchase costs from the breaching party FAR 49.402-7(a) (2022). Likewise, Government may also demand administrative costs FAR 49.402-7(b) (2022). This paper will focus on the judicial remedy under the FCA.

³⁸ See *The False Claims Act*, DEP'T OF JUST. (Jan. 14, 2021), <https://www.justice.gov/civil/false-claims-act>.

³⁹ Claims are defined to be "any request or demand for money or property, whether under a contract or otherwise and whether or not the U.S. government has title to such money or property, which is made to an officer, employee, or agent of the U.S. government." 31 U.S.C. § 3729(b)(2).

⁴⁰ See 31 U.S.C. § 3729(a)(1)(A)–(G). Even though the Government may not have suffered actual damage from the actor, the intent of the actor alone can be enough for the Government to seek civil penalties and damages. See *United States v. Honeywell Int'l Inc.*, 798 F. Supp. 2d 12, 19 (D.D.C. 2011) (stating "[A] subcontractor may be liable under § 3729(a)(1) even when it did not itself present any false claims to the government if it engaged in a fraudulent scheme that induced the government to pay claims submitted by the contractor.").

⁴¹ 45 C.F.R. § 2554.6 (2022).

⁴² 31 U.S.C. § 3730.

⁴³ "The term "*qui tam*" is derived from a Latin phrase, "*qui tam pro domino rege quam pro se ipso*," or "who pursues this action on our Lord the King's behalf as well as his own." CHARLES DOLY, CONG. RSCH. SERV. *QUI TAM: THE FALSE CLAIMS ACT AND RELATED FEDERAL STATUTES* 1 (Apr. 26, 2021).

⁴⁴ 31 U.S.C. § 3730; see 31 U.S.C. § 3730(e) for limitation in the type of private claims that can be brought.

⁴⁵ 31 U.S.C. § 3729(a)(1); 85 Fed. Reg. 37,004-10; 28 C.F.R. § 85.5.

⁴⁶ 31 U.S.C. § 3729(a)(1); *id.* § 3729(a)(3).

espionage attempts by the PRC against the U.S. defense supply chain system and critical infrastructure?⁴⁷

III. “RAPIDITY IS THE ESSENCE OF THE WAR”⁴⁸: THE CRITICAL NEED FOR A MULTI-DOMAIN APPROACH TO ENFORCING SECTION 889

To answer the above question, we must first assess the level of threat the PRC’s cyber operations pose to U.S. interests. To do so, this section first looks inward by providing an overlook at the vulnerability of the U.S. supply chain system against cyberattacks. Second, it reviews Congress’s and DoD’s assessment of the PRC’s unfair trade practices, including cyber espionage, against the American defense industrial bases (DIB) and its impact on U.S. national security. The section then turns to U.S. interests overseas by looking at how the PRC has jeopardized the unity of U.S. coalition partners through the expansion of fifth-generation (5G) technology. In light of these analysis, the section answers the above question: that relying on the FCA for Section 889 Part B enforcement is not enough to guard U.S. national security from Chinese state-sponsored cyber operations. In doing so, the section highlights the challenges in utilizing the FCA for Section 889 Part B.

A. *Domestic and International Risks posed by the PRC Cyber Operations and their Impact on U.S. National Security*

The risk of cyberattacks and espionage against U.S. defense interests are present both within and outside of the geopolitical boundaries of the U.S. This section explores the impacts of recent domestic cyberattacks and the vulnerability exposed in the U.S. supply chain system. It also looks to the responses by Congress and DoD to secure these vulnerabilities in the DIB, including measures against cyber threats posed by the PRC’s unfair trade practices. Lastly, the section turns to the global stage, using the expansion of 5G technology to show how the fragmented responses from U.S. coalition partners around the world have led to a weakened posture against the threat of Chinese cyber invasion.

1. *Threats and Responses against the U.S. Defense Supply Chain and Critical Infrastructure*

As cyberattacks are increasing in scale and complexity, protecting the U.S. defense chain and critical infrastructure is no longer an issue that can be overlooked.⁴⁹ Active interference by both governmental and non-governmental hackers has impacted the lives of many Americans in their day-to-day lives. For instance, in 2013, a group of non-government affiliated hackers gained access to approximately 40 million debit and credit card users’

⁴⁷ As of March 2022, the author is unaware of any Section 889 violations that have led to a contractual termination through the FAR or prosecution by the Department of Justice (DoJ) under the FCA.

⁴⁸ Sun Tzu, *supra* note 2, at 97.

⁴⁹ See e.g., CROWDSTRIKE, 2021 GLOBAL THREAT REPORT (2021). In a survey of over 2,200 senior IT consultants, nearly 50% of them had faced experienced supply chain attacks in 2020, compared to 32% in 2018. See Michael Sentonas, *Trust Erodes Amid Ransomware Growth: 2021 CrowdStrike Global Security Attitude Survey*, CROWDSTRIKE: BLOG (Dec. 7, 2021), <https://www.crowdstrike.com/blog/2021-crowdstrike-global-security-attitude-survey/>

information from the network of a popular retail chain, Target Inc.⁵⁰ The hackers in this case were able to gain access to the vendor's network by using the credential of a third-party HVAC contractor.⁵¹ More recently in 2021, Colonial Pipeline, a U.S. oil pipeline system that delivers 45% of the fuel used in the Eastern U.S.,⁵² was hacked by a cybercriminal hacking group from Northeast Europe known as DarkSide.⁵³ This group utilized a Virtual Private Network (VPN) to infiltrate the company's network to disrupt equipment.⁵⁴ The hack halted the pipeline operations for roughly a month, which led to a gas shortage in the Southeast U.S.⁵⁵ The gas shortage, in turn, resulted in distribution issues and panic buying.⁵⁶ To regain access to their system, Colonial Pipeline paid 75 bitcoins, roughly worth 4.4 million dollars in 2021, in ransom to the cyber hackers.⁵⁷ In all, these everyday examples show how fragile our supply chain system is against years of threats. It further validates the concerns raised by the DoD, those guarding our national security interests, and their pursuit to lower the risk of cyberattacks by the PRC to our supply chain risk management program in the most efficient manner possible.

The increase in Congress' and DoD's focus on supply chain risk management shows cybersecurity threats are a recognized matter of national security, rather than a simple inconvenience for the public masses. Concern over Chinese hacking and technology theft has been a ubiquitous topic in congressional hearings.⁵⁸ The National Defense Authorization Act for Fiscal Year 2022 shows the commitment of Congress to address some of these concerns by including numerous provisions dedicated to supplying chain security against foreign adversaries such as the PRC.⁵⁹ The provisions, for instance, include a new statutory requirement for the DoD to develop "capabilities to map supply chains and to assess risks to the supply chain for major end items"⁶⁰ and to reduce the reliance on, among other nations,

⁵⁰ Gregory Wallace, *HVAC Vendor Eyed as Entry Point for Target Breach*, CNN BUSINESS (Feb. 7, 2014), <https://money.cnn.com/2014/02/06/technology/security/target-breach-hvac/index.html>.

⁵¹ *Id.*

⁵² Cathy Bussewitz et al., *Colonial Pipeline Restarts Operations Days After Major Hack*, ASSOCIATED PRESS (May 12, 2021), <https://apnews.com/article/europe-government-and-politics-technology-business-938b33938fe3a750367fb1dc2f7ce6e0>.

⁵³ *Id.*

⁵⁴ Stephanie Kelly & Jessica Resnik-ault, *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, REUTERS (June 8, 2021), <https://www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/>

⁵⁵ Bussewitz, *supra* note 52.

⁵⁶ *Id.*

⁵⁷ See Press Release, Dep't of State, Department of Justice Seizes \$2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside (June 7, 2021), <https://www.justice.gov/opa/pr/department-justice-seizes-23-million-cryptocurrency-paid-ransomware-extortionists-darkside>. Though the Federal Bureau of Investigations was able to recover 63.7 bitcoins, it does not belittle the fact that the colonial pipeline was unable to operate until the ransom was paid to the hackers. *Id.* See also Kevin Collier & Pete Williams, *Feds Recover Millions from Pipeline Ransom Hackers, hint at U.S. Internet Tactic*, NBC NEWS (May 12, 2021), <https://www.nbcnews.com/tech/security/u-s-recovers-millions-pipeline-ransom-because-hackers-mistake-n1269889> (converting the 75 bitcoins to a dollar figure).

⁵⁸ *Supra* text accompanying note 18.

⁵⁹ National Defense Authorization Act for Fiscal Year 2022, Pub. L. No. 117-81, §§ 841–848, 135 Stat. 1541 (2022) [hereinafter FY22 NDAA].

⁶⁰ *Id.* § 841.

the PRC, to fulfill critical defense requirements.⁶¹ In a 2018 report, the DoD identified roughly 300 risks across sixteen sectors of the DIB and pointed out five areas that heightened supply chain risk to the DIB.⁶² In discussing industrial policies of competitor nations, one of the five areas highlighted by the DoD in the report, states the following:

“[b]y actively promoting the fusion of its military and civilian industrial and science and technology sectors, Beijing strives to reinforce the People’s Republic of China’s capabilities to build the country into an economic, technological, and military power while ensuring that overall control of these elements of national power remains firmly in the hands of the Communist Party of China.”⁶³

The DoD paints a gloom outcome in its report. Without additional protection, according to the DoD, the aggressive unfair trade practices of the PRC⁶⁴ will lead the nation towards overreliance on foreign resources to meet national security needs.⁶⁵ As a countermeasure to these threats, the DoD highlighted its current efforts to streamline the supply chain defense, such as the reorganization of the Section 809 panel,⁶⁶ increased workplace education to foster more efficient acquisition processes, as well as establishing a process to monitor the DIB per Section 1071(a) of the National Defense Authorization Act for FY 2018.⁶⁷ The DoD also recommended in its 2018 report that the U.S. seeks to diversify away from “politically unstable countries” by encouraging reengineering and increased qualification of new suppliers, as well as accelerating the growth of domestic STEM and critical trade skills.⁶⁸ In all, the recent statutory measures by Congress and the push for regulatory oversight by the DoD, coupled with the clear vulnerabilities within the DIB, shows the threat posed by the PRC’s aggressive cyber infiltration of the DIB should not be underestimated and requires a dynamic response.

2. Disjointed Response to Cyber Threats: How the Race to 5G is Fracturing the Bond Among the U.S. and its Coalition Partners

The impact of cyberattacks and cyber espionage reaches further than the geographical boundary of the U.S. The PRC, by using its national law to control its civilian industry, is

⁶¹ *Id.* § 847.

⁶² See Dep’t of Def., *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States: Report to President Donald J. Trump by the Interagency Task Force in Fulfillment of Executive Order 13806*, at 11 (2018). The sixteen defense sectors were divided up between “traditional sectors,” such as aircraft, munitions and missiles, shipbuilding, and space, and “Cross-cutting,” such as cybersecurity for manufacturing, electronics, and software engineering. *Id.* at 12. The five macro forces that the DoD identified as driving risk into the DIB included sequestration and uncertainty of U.S. Government spending, the decline of U.S. manufacturing base capabilities and capacity, deleterious U.S. Government business and procurement practices, industrial policies of competitor nations, and diminishing U.S. Stem and trade skills. *Id.* at 19–20.

⁶³ *Id.* at 35.

⁶⁴ Such practice includes state-sponsored price dumping, public subsidies, and intellectual theft. *Id.*

⁶⁵ See *id.* at 42.

⁶⁶ National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115-91, 131 Stat. 1283 (Dec. 12, 2017).

⁶⁷ See DEP’T OF DEF., *supra* note 62, at 54.

⁶⁸ See *id.* at 5.

weakening the ties among the traditional allies of the U.S. and its future partner nations through the global 5G technology expansion. 5G technology, simply put, increases the speed of data transfer and improves bandwidth in cellular networks over 4G technology.⁶⁹ Ever since its rollout in 2018, establishing a 5G network has quickly become the center of global attention.⁷⁰ The “Race to 5G” is crucial as 5G technology is projected to not only have commercial applications, but will also advance military operations in areas such as intelligence, surveillance, and reconnaissance (ISR) systems, command, and control (C2) capabilities, and more.⁷¹ Though the U.S. has finally taken the lead over 5G readiness,⁷² the current leading provider of 5G technology is Huawei, a Chinese multinational technology corporation, which captured 30% of the global market by the end of 2020.⁷³ While this fact alone would not be concerning, a significant national security concern should be raised for any nation utilizing Huawei’s 5G technology when paired with China’s National Intelligence Law.⁷⁴ Under the amended National Intelligence Law,⁷⁵ the PRC requires companies operating in the PRC, such as Huawei, to “grant intelligence officials the right to enter otherwise restricted facilities, examine private records, investigate and question personnel, and access or even requisition communications or transport equipment owned by companies or individual.”⁷⁶ This would mean that any consumer information, aggregate data, and other open-source information, as well as potentially confidential/national security sensitive

⁶⁹ See John R. Hoehn et al., Cong. Rsch. Serv., National Security Implications of Fifth Generation (5G) Mobile Technologies (2021).

⁷⁰ The top providers of 5G are from the PRC, the Republic of Korea, Japan, and the U.S. See CELLULAR TELECOMM. INDUS. ASS’N, THE GLOBAL RACE TO 5G (2018).

⁷¹ JOHN R. HOEHN ET AL., *supra* note 69. To that end, countries have also been broadening their radio frequencies to accommodate for 5G service distribution as well as instituting infrastructure policies, increasing industry investment, and increasing overall government support. See CELLULAR TELECOMM. INDUS. ASS’N, THE GLOBAL RACE TO 5G 3 (2018); Riley Davis, *What is Spectrum? A Brief Explainer*, CELLULAR TELECOMM. INDUS. ASSOC. (June 5, 2018), <https://www.ctia.org/news/what-is-spectrum-a-brief-explainer> (providing greater explanation on spectrum).

⁷² Cellular Telecomm. Indus. Ass’n, The Global Race to 5G: Spring 2019 Update 2 (2019).

⁷³ Meghan Bobrowsky et al., *Huawei, Ericsson or Nokia? Apple or Samsung? U.S. or China? Who’s Winning the 5G Races*, WALL ST. J. (Oct 12, 2021), <https://www.wsj.com/articles/huawei-ericsson-nokia-apple-samsung-u-s-china-winning-5g-race-1163400044>.

⁷⁴ National Intelligence Law of the People’s Republic (promulgated by the Standing Comm. Nat’l People’s Cong., June 27, 2017, rev’d Apr. 27, 2018, effective Apr. 27, 2018), art. 11, 2010 P.R.C. Laws 71.75 (China); *PRC National Intelligence Law (as amended in 2018)*, CHINA L. TRANSLATE, <https://www.chinalawtranslate.com/en/national-intelligence-law-of-the-p-r-c-2017/> (last visited May 4, 2024).

⁷⁵ Interestingly, this monumental amendment came in place in 2018, the same year in which 5G technology was globally rolled out. *Id.*; CELLULAR TELECOMM. INDUS. ASS’N, *supra* note 70.

⁷⁶ Murray S. Tanner, *Beijing’s New National Intelligence Law: From Defense to Offense*, LAWFARE (July 20, 2017), <https://www.lawfaremedia.org/article/beijings-new-national-intelligence-law-defense-offense>; see also “...the lines between the Chinese government and the Chinese Communist Party are blurred, if not totally erased. The lines between the Chinese government and Chinese state-owned enterprises, the same. The line between the Chinese government and ostensibly private companies, for all the reasons you described, and especially the line between lawful behavior and fair competition and lying and hacking and cheating and stealing.”

Open Hearing: Worldwide Threat Assessment of the U.S. Int’l Comm., Hearing Before the Select Comm. on Int’l of the U.S. S., 116th Cong., 60 (2019) (statement of Director of the Fed. Bureau of Investig., Christopher A. Wray).

materials, collected through Huawei 5G technology, could be accessed by the PRC and greatly compromise the national security of the U.S. and its allies.⁷⁷

The global market dominance by companies operating out of the PRC on the 5G frontier has already strained international relations among several key U.S. allies.⁷⁸ The most notable example of this dilemma on the global stage is the adaptation of 5G technology among the Five Eyes alliance.⁷⁹ In response to Huawei's aggressive market capturing and its role as the arm of the PRC, the U.S. has called for limiting Huawei's 5G expansion and other similarly situated PRC companies on the global stage.⁸⁰ This includes limiting U.S. military cooperation and intelligence sharing with countries that adopted Chinese 5G technology.⁸¹ In response to a question regarding U.S. interoperability with Five Eyes and Huawei technology, the then-Secretary of State Mike Pompeo stated the following:

“[I]f a country adopts [Huawei 5G technology] and puts it in some of their critical information systems, we won't be able to share information with them, we won't be able to work alongside them. In some cases, there's risk we won't even be able to co-locate American resources, an American embassy or an American military outpost.”⁸²

Though the Five Eyes alliance eventually aligned with the U.S. and implemented regulations or bans against Chinese 5G companies, they did not come easily⁸³ and those nations still face problems in domestic implementation.⁸⁴ However, other key international allies who traditionally have favorable diplomatic or economic ties with the U.S., such as Saudi Arabia,

⁷⁷ Weifeng Zhong, *China's Telecom Giants Are a Threat to Our Security*, THE DISPATCH (Dec. 16, 2021), <https://thedispatch.com/article/chinas-telecom-giants-are-a-threat/>.

⁷⁸ See also Secure 5G and Beyond Act of 2020, Pub. L. No. 116-129, 134 Stat. 223 (Mar. 23, 2020).

⁷⁹ See FIVE EYES INTEL. OVERSIGHT AND REV. COUNCIL, CHARTER OF THE FIVE EYES INTELLIGENCE OVERSIGHT AND REVIEW COUNCIL (2017). Generally, the Five Eyes alliance is a pact of military intelligence sharing among Australia, Canada, New Zealand, United Kingdom, and the U.S. that has been established since World War II. *Id.*

⁸⁰ See Julian E. Barnes & Adam Satariano, *U.S. Campaign to Ban Huawei Overseas Stumbles as Allies Resist*, N.Y. TIMES (Mar. 17, 2019), <https://www.nytimes.com/2019/03/17/us/politics/huawei-ban.html>.

⁸¹ Press Release, Robert Strayer, Deputy Assistant Secretary for Cyber and International Communications and Information Policy Bureau of Economic and Business Affairs, Progress on the 5G Security Campaign (July 21, 2020), <https://2017-2021.state.gov/briefings-foreign-press-centers/progress-on-the-5g-security-campaign/index.html>.

⁸² Interview by Maria Bartiromo with Michael R. Pompeo, Secretary of State (Feb. 12, 2019), <https://2017-2021.state.gov/interview-with-maria-bartiromo-of-mornings-with-maria-on-fox-business-network-3/index.html>.

⁸³ See e.g., Adam Satariano, *Britain Defies Trump Plea to Ban Huawei From 5G Network*, NEW YORK TIMES (Jan. 28, 2020), <https://www.nytimes.com/2020/01/28/technology/britain-huawei-5G.html> (stating that U.K. refused to ban Huawei 5G equipment despite a request from the U.S.). But see Press Release, Department for Digital, Culture, Media & Sport, National Cyber Security Centre & the Right Honorable Oliver Dowden CBE MP, Huawei to be Removed from UK 5G Networks by 2027 (July 14, 2020), <https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027> (stating the U.K. will stop buying Huawei 5G equipment as of 31 December 2020 and will be removed from U.K. 5G network by 2027 due to U.S. sanctions imposed on Huawei in May 2020).

⁸⁴ See Zoe Kleinman, *Why is Huawei Still in the UK?*, BBC (May 17, 2021), <https://www.bbc.com/news/technology-57146140> (stating that despite U.K.'s ban on Huawei 5G infrastructure, Huawei remains in close research partnership with over 30 U.K. universities).

Turkey, and Brazil, have decided to press ahead with adopting Huawei technologies for their 5G expansion, thereby further threatening U.S. interoperability on the global stage.⁸⁵

It is evident that the U.S. supply chain system, from HVAC to VPN, has critical cyber security vulnerabilities that the PRC can and will exploit to endanger U.S. national security. As the case of the 5G technology expansion shows, this threat has already impacted U.S. diplomacy and military alliances. Considering the scale and the catastrophic outcome these vulnerabilities can inflict on the U.S. defense supply chain and critical infrastructures, a sweeping regulation such as Section 889 was direly needed. Through Section 889, the U.S. will be able to protect its supply chain by removing Chinese telecommunication equipment and services that could be used as a tool for cyberattack and espionage by the PRC. However, in assessing whether Section 889 will be effective against this dire threat, we must determine whether the current model of Section 889 implantation allows for quick and responsive enforcement through the FCA, the primary judicial recourse for a Section 889 violation.

B. The Inadequacy of the FCA in Enforcing Section 889 Violations

The regulatory implantation of Section 889 has created significant hurdles and challenges for the successful enforcement of the statute through the FCA. Namely, the FCA is not responsive enough to enforce Section 889 due to the ambiguities present in the FAR regarding Section 889 and the lack of subject matter expertise by contractors to satisfy a dispositive element of an FCA claim. Likewise, the unlikelihood of finding reliable oversea whistleblowers who can identify the violations within these Chinese companies will hinder the effectiveness of the FCA in the face of Section 889 violations.

Section 889 Part B's broad requirement of "reasonable inquiry" into whether a contractor is "using" a covered technology will handicap enforcement through the FCA as it will cut against a terminal element of the statute. Under the FCA, the element of "knowingly" is defined as having "(1) ... actual knowledge of the [falsity]; (2) act[ing] in deliberate ignorance of the truth or falsity of the information; or (3) act[ing] in reckless disregard of the truth or falsity of the information, and no proof of specific intent to defraud is required."⁸⁶ In *U.S. v. Escobar*, the Supreme Court stated the FCA's requirement of scienter must be applied rigorously and should be enforced strictly.⁸⁷ The Court noted the basis for FCA liability is established when "the claim [by the defendant] does not merely request payment [from the government], but also makes specific representations about the goods or services provided."⁸⁸ This is problematic when it comes to enforcing Section 889 Part B's violation through the FCA.⁸⁹ As previously noted, currently, an offeror must self-certify whether they are using a CTES.⁹⁰ While comments from the public show general support for the reasonable inquiry standard utilized in these self-certifications, there have

⁸⁵ David Sacks, *China's Huawei is Winning the 5G Race. Here's What the United States Should do to Respond*, COUNCIL ON FOREIGN REL.: NET POLITICS (Mar. 29, 2021), <https://www.cfr.org/blog/china-huawei-5g>.

⁸⁶ 31 U.S.C. § 3729(b)(1). Moreover, there is no requirement to show that there was specific intent to defraud.

⁸⁷ See *Universal Health Services v. United States ex rel. Escobar*, 579 U.S. 176 (2016).

⁸⁸ See *id.*

⁸⁹ *Supra* Part II.B. on the discussion regarding the current Section 889 Part B certification model.

⁹⁰ *Id.*

been concerns regarding the lack of clarity on what constitutes a “use” of a CTES.⁹¹ This has led to confusion and many questions by defense contractors on the scope of the reasonable inquiry search.⁹² Under the scienter requirement, an ambiguous regulation could topple the Government’s FCA case.⁹³ An “honest [mistake] or incorrect [claims] submitted through mere negligence” is not enough to meet the scienter standard.⁹⁴ While not to say that an inference cannot be drawn *per se*,⁹⁵ by trying to hold an individual liable for an FCA violation through an ambiguous regulation, the Government puts itself in a weakened position. This is especially problematic for Section 889 Part B. Without much industry standard or guidance provided by the federal government, Section 889 Part B requires subject matter expertise that may be unavailable for many small businesses. This problem is exacerbated by the lack of clarity provided on what constitutes a “use” of covered equipment or services, as voiced by several contractors.⁹⁶ Consequently, without a clearer statutory or regulatory guideline, successfully holding defense contractors liable for violating the FCA will not only be a difficult challenge, but also a time-consuming approach.

In addition to the ambiguous regulatory language, the next challenge to successful utilization of the FCA is the heavy reliance of successful FCA cases on *qui tam* relators. As discussed earlier,⁹⁷ *qui tam* relators are FCA cases brought on by whistleblowers who know

⁹¹ The scope of what may constitute a “use” is broader than the federal contract. *See* July Interim Rule (stating “[t]his prohibition applies at the prime contract level to an entity ... regardless of whether that usage is in performance of work under a Federal contract.”).

⁹² Nat’l. Def. Indus. Assoc., *supra* note 14; *see also* Section 889: Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment: Webinar with GSA Business Lines, General Services Administration 12 (Sept. 10, 2020) (listing the numerous unanswered questions regarding “use” from the industry, such as whether a commercial sale of covered telecommunication equipment or service would constitute as use, or if an employee’s personal property of covered item constitutes use.). Perhaps the most telling of this frustration from the industry is best provided in whole:

“The rule does explain that “use” includes any kind of use, even if it is wholly unrelated to the performance of the federal contract. But it does not explain whether “use” includes the “commercial sale” of covered equipment. This will likely affect many of my customers who sell cameras produced by covered companies, but who themselves do not actually use those cameras. Likewise, the rule does not explain whether “use” includes the “installation” or “maintenance” or “testing” of covered equipment. Service providers may do all those things for customers and yet not “use” that equipment in their own supply chain. And in an extended era of working from home, the rule should clarify whether an “entity” uses covered equipment if one of its employees uses covered equipment while working from home. Likewise, it should clarify whether a company’s Bring Your Own Device (BYOD) policy, which allows employees to use their own devices to conduct company business, would amount to an entity’s use of the covered equipment.”

Clear Connection, Comment Letter on Federal Acquisition Circulars (FAC) Introduction and Small Entity Compliance Guide (SECG) (Oct. 26, 2020), <https://www.regulations.gov/comment/FAR-2020-0051-0034>.

⁹³ *United States ex rel. Complin v. N.C. Baptist Hosp.*, 818 Fed. Appx. 179 (4th Cir. 2020).

⁹⁴ *United States ex rel. Owens v. First Kuwaiti Gen. Trading & Contr. Co.*, 612 F.3d 724, 728 (4th Cir. 2010).

⁹⁵ *See United States ex rel. Phalp v. Lincare Holdings, Inc.*, 857 F.3d 1148 (11th Cir. 2017) (holding that while the ambiguity of the statute does not preclude a successful FCA claim, the relator must show whether the defendant actually knew or should have known that its conduct violated a regulation in light of any ambiguity at the time of the alleged violation.); *United States ex rel. Purcell v. MWI Corp.*, 807 F.3d 281 (D.C. Cir. 2015) (holding a defendant of FCA claim may still be found liable despite relying on a reasonable interpretation of an ambiguous statute if the defendant was previously warned from away from the interpretation it relied on).

⁹⁶ *Supra* text accompanying note 92.

⁹⁷ *Supra* Part II.B.

the false representation made by a government contractor. Once a whistleblower files their complaint, the Department of Justice (DoJ) can either intervene and litigate the suit on behalf of the relator or leave the suit for the whistleblower to pursue on their own. According to DOJ statistics, in the fiscal year 2020 alone, 63% of the FCA cases were *qui tam* and were responsible for 75% of the total dollars recovered.⁹⁸ While not a direct comparison, the U.S. Security and Exchange Commission (SEC)'s report on their whistleblower program gives a glimpse into overseas whistleblower participation.⁹⁹ In their report, SEC has noted that 11% of their whistleblower complaints for the fiscal year 2021 were submitted from abroad.¹⁰⁰ Of the roughly 1350 reports the SEC received overseas, 152 reports were from the PRC.¹⁰¹ Though this is an incredible 375% increase from the 32 reports the SEC received from the PRC in Fiscal Year 2019,¹⁰² this upward trend should not be considered a direct corollary to the likelihood of Chinese citizens or individuals located in the PRC acting as an FCA whistleblower for Section 889 Part B violations. First, even considering the upward trend, it must not be ignored that, in total, whistleblower claims filed in the PRC make up less than 5% of the total whistleblower claims filed in both Fiscal Year 2019 and 2021.¹⁰³ Second, the SEC does not distinguish whether these reports were regarding a foreign corporation or a U.S. domestic entity with an overseas operation in the PRC. This is an important distinction as the oversight concern of a Section 889 violation would naturally be heightened towards a foreign corporation, with its ability to shield its non-compliant activity in an overseas location, as opposed to a U.S. entity that is subject to greater scrutiny through U.S. laws and regulations. Likewise, the reports do not reveal whether the overseas whistleblowers were the U.S. or foreign nationals. This is also relevant as the U.S. will need to rely heavily on foreign nationals in these overseas locations to pursue an overseas FCA violation.¹⁰⁴ Most importantly, unlike an FCA violation, where the identity of the whistleblower will be

⁹⁸ CIVIL DIVISION, U.S. DEP'T OF JUST., FRAUD STATISTICS OVERVIEW - OCTOBER 1, 1986 - SEPTEMBER 30, 2020, (2020), <https://www.justice.gov/opa/press-release/file/1354316/download> [hereinafter DOJ FCA STATS]. Of all the new matters raised in fiscal year 2020, there were only 64 new matters from the defense sector, compared to the 573 matters brought under health and human services. *Id.* Regardless, it should not be ignored that of those 64 new matters, 35 matters were brought by a relator. *Id.*

⁹⁹ The SEC's whistleblower program was greatly amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank") of 2010, which modified the Securities Exchange Act of 1934. Through the amended Securities Exchange Act, the SEC has been bringing civil enforcement of federal securities law violations such as insider trading. *See* Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (July 21, 2010).

¹⁰⁰ U.S. SEC. AND EXCHANGE COMM'N, 2021 ANNUAL REPORT TO CONGRESS WHISTLEBLOWER PROGRAM 38 (2021). However, it should also be highlighted that this report does not disclose the nationality of those whistleblowers.

¹⁰¹ *Id.*

¹⁰² U.S. Sec. and Exchange Comm'n, 2019 Annual Report to Congress Whistleblower Program 33 (2019).

¹⁰³ *Compare id.*, with U.S. Sec. and Exchange Comm'n, 2021 Annual Report to Congress Whistleblower Program 38 (2021).

¹⁰⁴ An example of an overseas FCA recovery is a decade-long South Korean bid-rigging case that was uncovered through a whistleblower. *See* Press Release, Dep't of Just., Three South Korean Companies Agree to Plead Guilty and to Enter into Civil Settlements for Rigging Bids on United States Department of Defense Fuel Supply Contracts (Nov. 14, 2018), <https://www.justice.gov/opa/pr/three-south-korean-companies-agree-plead-guilty-and-enter-civil-settlements-rigging-bids>.

inevitably revealed once the case is unsealed by DoJ for litigation,¹⁰⁵ a whistleblower of an SEC complaint may still maintain their anonymity to the collection so long as they have attorney representation.¹⁰⁶ Protection for whistleblower identity is crucial to increase overseas relator participation for the FCA. However, the likelihood that a foreign national residing in the PRC would be willing to risk their lives to file an FCA claim is highly unlikely as evidenced by the PRC's brutal handling of recent Chinese whistleblowers who attempted to hold the PRC accountable for COVID-19 and human rights violations.¹⁰⁷

Though an argument could be made that the success of non-*qui tam* suits over *qui tam* is sufficient to rely on for enforcing Section 889 violations, to rely on non-*qui tam* suits alone for enforcement would be the very definition of “missed opportunities.” As shown above, *qui tam* suits made up 75% of the total dollars recovered in the fiscal year 2020, and according to the FCA statistics published by the DoJ, 55% of total suits brought under FCA since 1986 on behalf of the DoD.¹⁰⁸ As such, by failing to capitalize on the whistleblowers, the amount of FCA cases against Chinese cyber security threats will be cut by more than half. Therefore, we must look for ways to bolster Section 889 FCA prosecution, or in the alternative, we must educate and encourage the contractors to participate in a more thorough review of their supply chain from cyber threats.

IV. “[COUNTER] THE ENEMY’S POWER; FORCE HIM TO REVEAL HIMSELF”¹⁰⁹:

SOLUTIONS TO ENHANCE FCA LITIGATION AND TO ENCOURAGE

CONTRACTOR PARTICIPATION IN SECTION 889

Combating Section 889 Part B enforcement challenges to protect the defense supply chain with the tools currently available will be difficult unless the DoD figures out a way to get ahead of the problem by shifting from a reactive posture to a proactive stance against the threats of cyber security. In this section, three different proposals are offered to mend the issues identified previously, such as the lack of clarity in the reasonable inquiry standard and the lack of subject matter expertise by the industrial base. The first proposal, which draws inspiration from the Federal Rules of Civil Procedure (FRCP) Rule 26(g) and the DoD Cybersecurity Maturity Model Certification (CMMC) framework, would require the defense contractors to provide additional information in the self-certification to create a stronger basis

¹⁰⁵ 31 U.S.C. § 3730(b)(3).

¹⁰⁶ *Office of the Whistleblower: Frequently Asked Questions*, U.S. SEC. AND EXCHANGE COMM’N (Dec. 10, 2020), <https://www.sec.gov/whistleblower/frequently-asked-questions>.

¹⁰⁷ See e.g., Rebecca Wright et al., “Some are just psychopaths”: Chinese Detective in Exile Reveals Extent of Torture Against Uyghurs, CNN (Oct. 5, 2021), <https://www.cnn.com/2021/10/04/china/xinjiang-detective-torture-intl-hnk-dst/index.html> (recounting a statement of a human rights whistleblower stating that he “can never return to China – “they’ll beat me half to death,” he said. “I’d be arrested. There would be a lot of problems. Defection, treason, leaking government secrets, subversion. (I’d get) them all,” he said.”); Emily Feng, *Critics Say China Has Suppressed And Censored Information in Coronavirus Outbreak*, NPR (Feb. 8, 2020), <https://www.npr.org/sections/goatsandsoda/2020/02/08/803766743/critics-say-china-has-suppressed-and-censored-information-in-coronavirus-outbreak>.

¹⁰⁸ DOJ FCA STATS, *supra* note 98.

¹⁰⁹ Sun Tzu, *supra* note 2, at 24.

for the FCA's scienter requirement. The second proposal involves a mandatory third-party audit for a select group of contractors based on the contractors and the corporation's nationality and location of the contractor's performance as part of their Section 889 certification before their bids on certain government contracts with heightened security risk. The final proposal is to include a third-party audit as a favorable evaluation factor for select contracts to encourage the contractors to implement heightened scrutiny over their supply chain voluntarily.

A. Increasing the Amount of Information to be Provided in the Contractor Certification Process

This proposal's goal is to enhance the bases of a Section 889 FCA claim and thereby increase the odds of successful Government litigation by requiring additional information from offerors to substantiate their self-certification under the FAR. This section discusses how the FRCP and the current jurisprudence, as well as the DoD CMMC framework, can provide insights to overcome the difficulties discussed in Part III.B. in litigating an FCA violation by enhancing the reasonable inquiry standard. In doing so, the section also provides an analysis of both the strength and challenges of implementing this proposal.

The current structure of the certification process under the FAR lacks the appropriate depth and fails to set up future FCA litigations for success. Under FAR section 4.2105, contractors must self-certify that they are not using a CTES for all solicitations for contracts.¹¹⁰ As discussed in Part II.B, this annual certification is made electronically after the contractors have conducted a "reasonable inquiry" to determine whether they had "used" a CTES.¹¹¹ Under *U.S. v. Escobar*, without being able to show that the contractor had knowingly violated the statute or the regulation, the likelihood of prevailing on an FCA litigation is low for the government as it will have failed to satisfy this scienter requirement.¹¹² As such, greater efforts must be made to bring additional context and structures to clarify the standard that should be used by the contractors before making their Section 889 certifications. By providing so little guidance and definition on what constitutes "use" of CTES, in addition to other problematic portions of Section 889, the U.S. is exposing itself to unnecessary risk that can be mitigated by creating a better standard for what would satisfy this reasonable inquiry standard.

Rule 26(g) of the FRCP regarding e-discovery can provide some insights on crafting such a standard. The term, reasonable inquiry, is also found under Rule 26(g) of FRCP.¹¹³ Generally stated, under Rule 26(g), an attorney is required to make a reasonable inquiry in response to every discovery request and response.¹¹⁴ Similar to FAR subsection 52.204-25, at a cursory view, the definition of reasonable inquiry in Rule 26(g) is uncomplicated. For example, under Rule 26(g), an attorney, concerning a disclosure, must make a reasonable

¹¹⁰ *Supra* text accompanying note 27.

¹¹¹ See July Interim Rule, 42666; see also GEN. SERV. ADMIN., SAM RELEASE NOTES BUILD 2020-10-24, at 3 (Oct. 24, 2020). However, a contractor would still be required to submit an "offer-by-offer" representation if they had represented that they do use the covered telecommunication equipment or service. *Id.*

¹¹² See *Universal Health Services*, 579 U.S. 176 (2016).

¹¹³ Fed. R. Civ. P. 26.

¹¹⁴ *Id.*

inquiry to ensure that the disclosure is “complete and correct as of the time it is made.”¹¹⁵ However, this simple standard for discovery becomes much more nuanced through case laws and in practice. Discussions regarding discovery have risen to prominence in light of the increased amounts of electronically stored information (ESI) involved in litigations due to society’s greater reliance on computers, e-mails, and other digital means to store and transmit data.¹¹⁶ In balancing out whether Rule 26(g) discovery obligations were met, federal courts have used the totality of circumstances standard to determine whether the counsel has “reasonably inquired” to satisfy the rule.¹¹⁷ While there is no hard and firm factors test has been established to determine whether a reasonable inquiry was made in response to a discovery request, the Northern District of Iowa has looked at the following factors on determining whether that standard was met:

“(1) the number and complexity of the issues; (2) the location, nature, number, and availability of potentially relevant witnesses or documents; (3) the extent of past working relationships between the attorney and the client, particularly in related or similar litigation; and (4) the time available to conduct an investigation.”¹¹⁸

While not a perfect solution, the above factors are a valuable resource that provides a primitive guideline on how to fortify the Section 889 certifications without suffocating the contractors with overwhelming requirements. By combining these factors with other pre-existing standards implemented to safeguard U.S. cyber security, such as the CMMC, enforcing Section 889 through the FCA will have one less hurdle in ensuring that those who compromise the defense supply chain will have to face a hefty price for their transgressions.

Requiring additional information from contractors to protect sensitive national security information is not a novel concept.¹¹⁹ Likewise, protecting the integrity of the DIB through the Section 889 certifications should not be treated any differently. The CMMC, which is a DoD program that will be fully implemented by 2025,¹²⁰ requires contractors to show cyber security measurement compliance before bidding on DoD contracts.¹²¹ Depending on the level of security required for the contract, under the CMMC framework, the contractor may conduct an annual self-certification or a triennial third-party

¹¹⁵ Fed. R. Civ. P. 26(g)(1)(A).

¹¹⁶ See Patrick Oot, Anne Kershaw & Herbert L. Roitblat, *Mandating Reasonableness in a Reasonable Inquiry*, 87 Denv. U. L. Rev. 533 (2010).

¹¹⁷ “The duty to make a “reasonable inquiry” is satisfied if the investigation undertaken by the attorney and the conclusions drawn therefrom are reasonable under the circumstances. It is an objective standard similar to the one imposed by Rule 11.” FED. R. CIV. P. 26 Notes of Advisory Committee on Rules – 1937. According to the advisory note, in making the inquiry, “the attorney may rely on assertions by the client and on communications with other counsel in the case as long as that reliance is appropriate under the circumstances. Ultimately, what is reasonable is a matter for the court to decide on the totality of the circumstances.” *Id.*

¹¹⁸ St. Paul Reinsurance Co. v. Commercial Fin. Corp., 198 F.R.D. 508 (N.D. Iowa 2000).

¹¹⁹ See DFARS 252.204-7021 (2020); CMMC FAQs, OFF. OF THE UNDER SEC’Y AND DEF., ACQ. AND SUSTAINMENT, <https://web.archive.org/web/20210728205354/https://www.acq.osd.mil/cmmc/faq.html> (last visited May 4, 2024).

¹²⁰ DFARS 252.204-7021 (2020).

¹²¹ The creation of the CMMC was a response to an increased threat against defense supply chain management and defense industrial base. See OFF. OF THE UNDER SEC’Y AND DEF., ACQ. AND SUSTAINMENT, *supra* note 119.

certification.¹²² However, unlike Section 889 self-certification, CMMC's self-assessment utilizes scoping guidance and provides the contractors with a detailed self-assessment guide.¹²³ The scoping guidance directs the contractors to target which technologies, systems, and people should be included in the self-assessment.¹²⁴ After establishing the scope, the contractors will use the self-assessment guide which will provide information on how to self-access each CMMC practice area by directing the users through domains of their systems that should be reviewed.¹²⁵ Within each of the domains, the guide suggests potential assessment methods and objects by describing what should be examined, which personnel should be interviewed, and how the system should be tested.¹²⁶ By providing clear instruction and resources, the CMMC self-assessment and certification process on its face has managed to maintain both a streamlined approach as well as prepare the grounds for a successful FCA litigation.¹²⁷

Like the CMMC certification model, Section 889's self-certification method can provide the contractors with streamlined guidance that will vary in its depth of analysis by the degree of national security implications involved with the contract. For instance, for projects with minimal to no involvement with national security matters, the annual certification could require the contractor to conduct a search based on the appropriate scope level as described by a detailed self-assessment guideline. Currently, the General Services Administration (GSA) has already published a Section 889 Part B compliance decision tree authored by their Supply Chain Risk Management (SCRM) review board.¹²⁸ Though this document is rudimentary, and no regulatory rule mandates its use, requiring the contractors to certify the use of the decision tree could provide greater leverage for a successful FCA litigation. As the national security implication of a contract rises, the certification can require a greater amount of disclosure and in-depth search as laid out by the Section 889 self-assessment guideline. In this scenario, like the CMMC process, only the contractors who have provided the requisite amount of information for the certification may compete for the contracts requiring heightened security. Such disclosure could include some of the factors

¹²² *CMMC FAQs*, *supra* note 119. Whether a contractor needs to engage in self-assessment, or a third-party review, depends on the level on which level of security they required is based on the level of assessment the contract required. *CMMC Model*, OFF. OF THE UNDER SEC'y AND DEF., ACQ. AND SUSTAINMENT, <https://web.archive.org/web/20211104225716/https://www.acq.osd.mil/cmmc/model.html> (last visited May 4, 2024).

¹²³ Off. of the Under Sec'y and Def., Acq. and Sustainment CMMC Self-Assessment Scope (2021) [hereinafter CMMC Self-Assessment Scope]; Off. of the Under Sec'y and Def., Acq. and Sustainment, CMMC Self-Assessment Guide Level 1 (2021) [hereinafter CMMC Self-Assessment Guide].

¹²⁴ See CMMC Self-Assessment Scope at 2.

¹²⁵ The categories include access control, identification and authentication, and physical protection, and more. See CMMC SELF-ASSESSMENT GUIDE at iii.

¹²⁶ It also offers other considerations to be assessed as part of the self-certification and provides key references to be linked back to the relevant FAR or National Institute of Standards and Technology (NIST) provision. *E.g.*, *id.* at 44.

¹²⁷ *E.g.*, Shardul Desai et al., *CMMC 2.0 Simplifies Requirements But Raises Risks for Government Contractors*, HOLLAND & KNIGHT (Dec. 8, 2021), <https://www.hklaw.com/en/insights/publications/2021/12/cmmc-2-simplifies-requirements-but-raises-risks>.

¹²⁸ SCRM REVIEW BOARD, SCRM CRITERIA FOR SECTION 889 PART B (Aug. 13, 2020), https://www.gsa.gov/cdnstatic/SCRM%20review%20board%20889%20PART%20B%20Rubric_20200901.pdf.

utilized in FRCP rule 26(g) analysis, such as describing the scope of the search by detailing the locations searched and the equipment examined, individuals interviewed, the method of the search, and description of any internal policy utilized by the contractor to ensure that they will not be utilizing CTES. The additional benefit to this approach is that it would standardize the industry review process for Section 889, thereby allowing the contractors to cross-share information on how to conduct these reviews efficiently and effectively. It would also create stronger bases for the FCA's scienter requirement since the additional clarity will better define the regulation's standard to imbue actual knowledge on potential violators.

In assessing the positives and the challenges of the above proposal, the crux of the issue lies in the subject matter expertise of both the contractor and the contracting team. A positive of this approach is that it is forward-leaning in multiple ways. First, it creates additional opportunities for the contractors to ensure that the CTES is not being supplied to the government agencies or is being used by the contractors themselves. It also sets up future FCA litigation for success by clarifying the ambiguity that lies in the current Section 889 language: namely, the standard for what a reasonable inquiry may include and the "use" standard.¹²⁹ However, the success in implementing this proposal lies in recognizing the diversity of our contractors. It would be ignorant to overlook the fact that one of the primary purposes of the federal acquisition system is to create a greater opportunity for small businesses to contract with the federal government.¹³⁰ The likelihood that these small businesses will have the resource, let alone the subject matter understanding, or the time, to be able to successfully audit and thoroughly articulate their justification for their Section 889 certification is low.¹³¹ Even with the larger businesses, as is the case for attorneys faced with the daunting task of meeting their discovery obligation over the ever-increasing amount of data produced from their clients,¹³² it will be a tall order for these companies to properly catalog and keep up with the latest technology as well as keeping track of all the new fiduciaries of the covered entities.¹³³ As such, this proposal, if it fails to strike a healthy balance between risk and reward of a thorough assessment guide, will more likely than not lock out both small and larger businesses from bidding for government contracts involving heightened national security implications.

¹²⁹ See *supra* notes 91-92.

¹³⁰ Steven L. Schooner, *Desiderata: Objectives for a System of Government Contract Law*, 11 PUB. PROCUREMENT L. REV. 103 (2002).

¹³¹ Rural Wireless Ass'n, *supra* note 28.

¹³² See eDiscovery Market by Component (Software (Processing, Review and Analysis, Identification, Preservation and Collection, and Production and Presentation) and Services), Deployment Type, Organization Size, Vertical, and Region - Global Forecast to 2027, MARKETS AND MARKETS, <https://www.marketsandmarkets.com/Market-Reports/e-discovery-market-11881863.html> (last visited May. 4, 2024) (discussing that eDiscovery market size is projected to grow from USD 11.2 billion in 2022 to USD 17.1 billion by 2027, at a Compound Annual Growth Rate (CAGR) of 8.7%).

¹³³ "We object to any interpretation or comments intended to expand the scope of the "reasonable inquiry" requirement, which would place a substantial burden on government contractors to the point of being impracticable." Comput. Tech. Indus. Assoc., Comment Letter on Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment (FAR Case 2019-009) (Sept. 14, 2020), <https://www.regulations.gov/comment/FAR-2019-0009-0053>.

B. Requiring a Third-Party Audit for Contractors with a Higher Risk of Violating Section 889

If a more stringent self-assessment guide alone is not enough to effectively enforce Section 889 without over-burdening the defense industry, what other options are possible? This approach requires potential offerors to use a third-party auditor before being able to compete for government contracts. To ease the burden on the contractors as well as the contracting bodies, a third-party audit would not be required of all contractors. Rather, it will only be required from prime contractors located overseas or prime contractors that are operated or owned by a foreign government or have legal obligations similar to the PRC's National Intelligence Law to a foreign government. This section explores why a third-party audit is needed and further discusses the type of contractors that would be the target demographic for the audit.

1. The Need for a Third-Party Audit in Section 889 Implementation and Enforcement

While self-certification would be the less taxing and time-efficient option over requiring a third-party audit process, a third-party audit may be necessary to ensure that the contractors are meeting the requirements of Section 889 Part B. A comparable case study can be found in the genesis of DoD's CMMC framework. CMMC was created to protect federal contracting information that was exposed through the weakness within the defense supply chain management.¹³⁴ Much like Section 889, the CMMC's goal is to protect controlled classified information from being leaked through the DIB.¹³⁵ This is not to say there were not any protections previously. A plethora of regulations and statutory requirements to combat these concerns were in place before 2019 such as the National Institute of Standards and Technology cyber security framework.¹³⁶ However, an audit by the DoD Inspector General (IG) revealed that relying on self-certification from the contractors has failed to effectively implement the much-needed security measures.¹³⁷ In response to these challenges, the DoD has implemented the CMMC which, along with self-certification, includes a mandatory third-party assessment and certification for contracts with heightened national security implications.¹³⁸ The CMMC's cautionary tale teaches a valuable lesson; relying solely on self-certification to ensure that our supply chains are free from a CTES is likely to lead to an

¹³⁴ See HEIDI M. PETERS, CONG. RSCH. SERV., DEFENSE ACQUISITIONS: DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK (2020), <https://crsreports.congress.gov/product/pdf/R/R46643/2>.

¹³⁵ *Id.* at 5.

¹³⁶ See *id.* at Appendix A & B (providing a list of U.S. regulatory measures and NIST publications in place to mitigate cybersecurity risk.).

¹³⁷ See Inspector General, U.S. Dep't of Def., Report No. D ODIG-2019-105 Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems (July 23, 2019). In the report, the DoD IG pointed out the lack of oversight by the DoD contracting offices and the requiring activities on how their contractors were storing CUI or where these CUI were being stored. *Id.* at 20–22. The DoD IG also highlighted that both the contracting offices, as well as the contractors, have failed to take appropriate actions regarding spillage of classified information. *Id.* at iii.

¹³⁸ HEIDI M. PETERS, CONG. RSCH. SERV., DEFENSE ACQUISITIONS: DOD'S CYBERSECURITY MATURITY MODEL CERTIFICATION FRAMEWORK 1 (2020), <https://crsreports.congress.gov/product/pdf/R/R46643/2>.

unsatisfactory outcome. As such, a hybrid model requiring self-assessment as well as a third-party audit system would be the necessary step forward to ensure that the goals of Section 889 are met.

A third-party audit process, in conjunction with an updated self-certification, would further Section 889 enforcement. Though it seems like a simple concept in the definition provided in the statutory language of Section 889,¹³⁹ ambiguity still exists in defining what constitutes telecommunication equipment or service. For instance, there is no specific list that states what type of equipment or service would fall within the scope of the definition to help the lay small-business owner to know which of their equipment may violate Section 889.¹⁴⁰ Likewise, a contractor may not realize the difference between covered equipment and services as opposed to “excepted equipment and services.”¹⁴¹ Regardless of these challenges, it is still the contractor’s responsibility to identify this equipment and services. Ultimately, however, it will be the U.S. supply chain security that will bear the risk should the contractor fail to properly vet their equipment or services. The key, therefore, is to focus on educating the industries rather than focusing on punishing the contractors for failing to understand Section 889. By availing proper resources to the contractors, such as government-certified third-party subject matter experts who have been vetted by the U.S. government to ensure their proficiency in applying Section 889 criteria, we can expect a higher rate of compliance from the defense industries. In conducting their third-party audit for CMMC, the DoD has entered an exclusive contract with a non-for-profit organization that will, in turn, train other private entities to conduct CMMC third-party certification exams.¹⁴² These trained bodies, known as CMMC Third Party Assessment Organization (C3PAO), will conduct a third-party audit for contractors seeking to enter a contract with the DoD on contracts with heightened national security implications. Like the CMMC, Section 889 Part B compliance can be streamlined by having a third-party audit system with trained subject matter experts who would conduct Section 889 compliance checks for contractors seeking to bid on certain DoD contracts. This program would also benefit the DoD by establishing a robust industry standard utilized by both the contracting activity and by the contractors for Section 889 Part B compliance and thereby further secure the DoD supply chain from foreign adversaries.

Another challenge for the contractors that could be cured by a third-party audit system is keeping track of the numerous identities of subsidiaries and affiliates of the covered entities. Under Section 889, the contractors are not only responsible for ensuring that they are not utilizing CTES from the five Covered Entities, but they must also ensure that they are not utilizing parts and services from the subsidiaries and affiliates of said entities.¹⁴³ This has caused confusion among the agencies, as evidenced by the Q & A response by GSA and U.S.

¹³⁹ Appendix B.

¹⁴⁰ And understandably so, as it would be near impossible to document every single telecommunication equipment that contains parts from the covered entities.

¹⁴¹ Excepted equipment and service is defined in Appendix A. Already, there has been a call to clarify what “excepted equipment” means and the scope of these exceptions. See Council of Def. and Space Indus. Ass’n, Comment Letter on Federal Acquisition Regulation: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment 4 (FAR Case 2019-009), <https://www.regulations.gov/comment/FAR-2019-0009-0064>.

¹⁴² CMMC-AB *Frequently Asked Questions*, CMMC ACCREDITATION BODY, <https://cyberab.org/FAQ>.

¹⁴³ FY19 NDAA, § 889(f)(3)(B).

Agency for International Development (USAID). In response to the industry's question of whether a list of subsidiaries and affiliates will be provided, GSA responded that neither the FAR nor the agency has such a list available for the contractors.¹⁴⁴ When USAID was asked a similar question, it responded that while it does not maintain such a list, the Department of Commerce (DoC) maintains a list of affiliates and subsidiaries of covered Chinese companies.¹⁴⁵ The list being referred by USAID, however, is not for Section 889. Rather, the purpose of the "Entity List" is to identify foreign persons and entities that are required to apply for certain licenses to export or transfer specific items for reasons of national security and/or foreign policy interests.¹⁴⁶ While this list would be a helpful secondary resource, it is not a controlling list for Section 889.¹⁴⁷ As such, without a definitive guide for the contractors to keep track of all of the covered entities' domestic and overseas subsidiaries and affiliates, there will be inconsistent and ineffective results in implementing Section 889. Here, a third-party audit system like the CMMC's C3PAO can fill in this critical gap in knowledge by focusing specifically on the five Covered Entities and keeping up with their corporate identity across the world. By having organizations that can focus solely on Section 889 Part B compliance, both the contractors and individual agencies can benefit by having access to the most up-to-date knowledge of the subsidiaries and affiliates of covered entities and ensuring that their telecommunication equipment or services would not involve using parts from said subsidiaries and affiliates.

2. Requiring a Third-party Audit for Overseas Prime Contractors and Certain Domestic Prime Contractors

To balance out the competition interest of the federal acquisition system and safeguard the U.S. supply chain system, this approach would require a third-party audit only from contractors with ties to a foreign government that is bidding on contracts with heightened national security implications. Under this system, there would be a tiered approach based on the amount of national security implication of the contract requirement at hand. For instance, contracts with little or no national security implication would only require a self-assessment as described in Part IV.A, while a contract with higher national security implication would require a more thorough third-party assessment. Specifically, the third-party audit would be only required from overseas prime contractors with any ties or obligation to a foreign government, or domestic prime contractors with greater than 50%

¹⁴⁴ Section 889: Prohibition on Certain Telecommunications and Video Surveillance Services or Equipment: Webinar with GSA Business Lines, General Services Administration 12 (Sept. 10, 2020).

¹⁴⁵ U.S. Agency for International Development Section 889 Task Force Section 889 Frequently Asked Questions (FAQs) for Contractors and Recipients of USAID award, USAID (Oct. 23, 2020).

¹⁴⁶ *Entity List*, BUREAU OF INDUS. AND SEC., U.S. DEP'T OF COM., <https://www.bis.gov/articles/entity-list/>.

¹⁴⁷ However, this list is useful in assessing how many foreign subsidiaries of the Covered Entities have been discovered each year. For instance, since making its first appearance on the list in 2019 with sixty-eight non-U.S. affiliates, The DoC added another forty-six to the list just within three months of the initial debut, and in 2020, added another thirty-eight non-U.S. affiliates of Huawei to the list. Addition of Huawei Non-U.S. Affiliates to the Entity List, the Removal of Temporary General License, and Amendments to General Prohibition Three (Foreign-Produced Direct Product Rule, 85 Fed. Reg. 162, 51,596–51,629 (Aug. 20, 2020) (to be codified at 15 C.F.R. pt. 736, 744, and 762)).

ownership stake by a foreign entity with ties or obligation to a foreign government.¹⁴⁸ It would also require that the prime contractors subject to this rule would also compel any of their subcontractors to conduct the enhanced self-assessment process under Part IV.A. By requiring that a contractor with ties with all foreign governments rather than just the PRC participate in a third-party audit, this approach ensures that foreign governments who has less stringent standards for cyber security will not inadvertently expose the U.S. supply chain system to cyber infiltration from the PRC.¹⁴⁹

Requiring disclosure of foreign associations from contractors or requiring oversight over subcontractors from the prime contractor is not a new concept and will further the effectiveness of Section 889. This kind of compulsory disclosure from contractors regarding their association with a foreign government is not unprecedented.¹⁵⁰ As such, assuming there is a significant overlap between the type of contracts that falls under the FY19 NDAA mandate and the contracts with heightened national security implications, the data regarding ownership and relation to foreign government should be readily available for the majority of the contracts that would require the third-party audit. Likewise, under FAR 42.204-25, the prime contractors are still required to conduct a reasonable inquiry of the subcontractors being utilized under their contract. By placing a greater requirement on the prime contractor to ensure a more thorough self-assessment of their subcontractors and requiring the prime contractor to make affirmative representation to the Government of the subcontractor's compliance, it will weaken claims of regulatory ambiguity in case of future breaches of Section 889. In addition, the Government will be in a superior position to enforce Section 889 through the FCA on both the prime and the subcontractor.

Focusing specifically on contractors with obligations with a foreign government where the risk of Section 889 noncompliance is the strongest would lessen the burden on the other contractors on having to participate in a third-party audit. While the more absolute method of ensuring Section 889 Part B compliance would be to require a third-party audit for all contractors regardless of national origin and the types of contracts, such a request to smaller businesses may be cost prohibitive, overly burdensome, and cause undue delay in fulfilling government needs.¹⁵¹ As such, by surgically targeting the contractors with a

¹⁴⁸ Although the ideal solution would require all contractors to be submitted to a third-party vetting, as noted by comments made by the defense industrial base, such a measure may cripple the contracting process and cause undue distress. *e.g.*, MARKETS AND MARKETS, *supra* note 133 (noting a contractor's rejection of requiring an internal or a third-party audit to enforce Section 889). As such, considering such concerns, this proposal limits the scope to those who are most likely to be at risk of violating Section 889 Part B.

¹⁴⁹ David Sacks, *supra* note 85.

¹⁵⁰ For instance, under FY19 NDAA, contractors must disclose any obligation to foreign government prior to entering certain contracts with the DoD. See FY19 NDAA § 1655. (Establishing that the DOD may not use a product, service, or system procured or acquired relating to information or operational technology, cybersecurity, an industrial control system, or weapons system provided by a person unless that person makes a series of disclosures regarding potential obligations to a foreign government.).

¹⁵¹ For instance, the CMMC recently went under a structural revision that simplified the framework and created waiver process in response to industry hardship and difficulty in implementing its initial model. See CMMC FAQs, OFF. OF THE UNDER SEC'Y AND DEF., ACQ. AND SUSTAINMENT, <https://web.archive.org/web/20210728205354/https://www.acq.osd.mil/cmmc/faq.html> (last visited May 4, 2024) (stating CMMC 2.0 was implanted to reduce costs for small businesses; increase trust in the CMMC assessment ecosystem; and to clarify cybersecurity requirements to other federal requirements and commonly

heightened risk of cyber security breach, this solution seeks to provide a pragmatic option that seeks to limit the risk without gridlocking the entire government acquisition process. However, like the enhanced self-assessment, requiring a third-party audit may still be too cost-prohibitive for certain contractors who would be mandated to participate, leading to a decrease in competition. This could also be especially problematic for requiring activities seeking to fulfill contracts in remote areas that would most likely only be fulfilled by an overseas contractor, leading to an increase in the contract price or contractor unavailability.

C. Encouraging the Contractors to Utilize the Third-Party Auditors Through FAR-based Incentives

Under this model, when allowed by the structure of the award process, an additional FAR Part 15 clause would be added to mandate a third-party audit as a favorable evaluation factor for contracts involving heightened national security implications, such as cybersecurity or a weapons system. For instance, in a negotiated procurement, as a technical evaluation factor, a factor could be designated as a Section 889 Part B compliance. Under this factor, the contractor that has received a favorable certification from a third-party Section 889 Part B compliance auditor would receive a higher rating than a contractor that did not conduct a third-party review and relied on the self-assessment process alone. Likewise, in a simplified acquisition process, the contracting officer could be required to consider a third-party audit to be a favorable factor in awarding a contract.

The benefit of this approach is that it will encourage the individual contractors to utilize the third-party auditors by incentivizing their use rather than forcing their use, which could have a chilling effect on the competition among the DIB. While this method would still require the creation of a CMMC-AB like body that will oversee that qualified subject matter experts are available, this would be the least intrusive approach of the three proposed courses of action. Unlike the previous two proposals, which require the contractors to participate in an enhanced self-certification process or require a third-party audit for a certain group of contractors, this proposal does not demand any action on part of the contractor. Rather, it is purely an incentive model that an offeror may utilize should they seek to get a higher rating on their quote or a proposal. Likewise, unlike the second proposal which would necessitate a third-party audit, this approach falls more in line with the existing interim rule which states that a third-party audit would not be required to fulfill the reasonable inquiry threshold.¹⁵² The ultimate goal of this approach is to incentivize the contracting community at large to voluntarily participate in a third-party audit so that it can become the industry standard. This would benefit both the government and the contractors in Section 889 Part B compliance and still strengthen the scienter element against an FCA violation like the other two proposals.

However, the challenge with this approach lies in the participation rate of the contractors and its inapplicability in certain contract award processes. For instance, this approach would not be applicable under a FAR part 14 sealed bidding procedure, which does

accepted standards.) For more information on the previous model, CMMC 1.0, and the difference between the two models, see *CMMC Model*, OFF. OF THE UNDER SEC'Y AND DEF., ACQ. AND SUSTAINMENT, <https://www.acq.osd.mil/cmmc/model.html> (last visited Mar. 31, 2022).

¹⁵² FAR 52.204-25 (2021).

not consider any evaluation factors and focuses solely on price.¹⁵³ Likewise, this model would be ineffective in promulgating a more robust Section 889 Part B compliance in a Lowest Price/Technically Acceptable (LPTA) award structure¹⁵⁴ as its incorporation as a factor in an LPTA would be essentially mandating the contractors to be subjected to a third-party review. This method could also limit competition by discouraging certain contractors from submitting a bid due to the initial cost associated with commissioning a third-party audit and the time necessary to conduct the audit. Lastly, offerors may elect not to use a third-party audit even if they would be awarded positive evaluation factors should the offerors determine the benefits from the factor would be outweighed by the price, the time to process the audit, or the time or the cost of implanting the changes the audit may require receiving the certification.

V. IN CONCLUSION: “HE WHO CAN MODIFY HIS TACTICS IN RELATION TO HIS OPPONENT AND THEREBY SUCCEED IN WINNING, MAY BE CALLED A HEAVEN-BORN CAPTAIN.”¹⁵⁵

The annual cost to the U.S. economy by counterfeit goods, pirated software, and theft of trade secrets amounts up to 600 billion dollars and the PRC stands at the helm of this operation.¹⁵⁶ In the face of rising cyberattacks and espionage from the PRC, regulations such as Section 889 are necessary for the U.S. to guard its defense supply chain and its alliance with current and future partner nations. As this article identified, however, there are significant challenges regarding enforcing Section 889 Part B through the FCA due to the inherent ambiguity in the regulatory language and the lack of contractor knowledge base.

To overcome this challenge, as Sun Tzu noted, we must be willing to modify our tactics. The first proposal in this article sought to create a more robust FCA litigation process by bolstering the self-assessment system through incorporating elements from the FRCP rule 26(g) and the CMMC’s self-assessment process. The second approach involved mandating a third-party audit against bidders of select contracts who are most likely to incur Section 889 violations. The third proposal incentivized a voluntary third-party audit by incorporating the audit to be a favorable factor under the FAR in certain contracting models. Though each proposal has its strengths, they also have its challenges which are mainly driven by the cost and time it would take to conduct such reviews, possibly resulting in a chilling effect on the DIB’s competition and the increasing procurement acquisition lead time. Other challenges included the lack of technical expertise by the contractors to be able to keep up with the ever-

¹⁵³ In fact, a third-party vetting and its associated costs may even price out contractors who utilized third-party vetting and built in the cost of the vetting to the offer from being competitive against an offeror who used self-assessment in this model. However, the likelihood of a sealed bidding process being utilized for a contract with heightened national security implications, such as cybersecurity or operational technology, is low as the complexity behind such contracts would mandate more than price-related factors and would warrant discussions during the bid process. See *Racal Filter Technologies, Inc.*, B-240579, 90-2 CPD ¶ 453 (Comp. Gen. Dec. 4, 1990).

¹⁵⁴ LPTA is a source selection process that defines best value as the any technically acceptable proposal with the lowest price. See FAR 15.101-2 (2021).

¹⁵⁵ Sun Tzu, *supra* note 2, at 52.

¹⁵⁶ FED. BUREAU OF INVESTIGATION, EXECUTIVE SUMMARY CHINA: THE RISK TO CORPORATE AMERICA (2019).

evolving technologies and the growing numbers of subsidiaries and affiliates of the companies that are sponsored by the PRC. Likewise, the contractors, despite being given an incentive to engage in third-party review, may still be hesitant to do so for economic reasons.

Perhaps the ideal approach would be a hybrid model of all three proposals; requiring a more robust self-assessment from all government contractors and to require a third-party audit system for contractors displaying the greatest risk of Section 889 Part B violation, and incentivizing contractor participation in a more vigorous Section 889 reviews. Regardless of what the right approach may look like, one thing remains clear; a meaningful Section 889 Part B enforcement will not take place unless greater clarity and guidance are provided to the DIB. There must be a way to not only increase enforcement of Section 889 through litigation but also to empower the DIB through education and incentives. By shifting the focus from a reactive approach to taking a proactive measure, the U.S. government can harness the power of Section 889 to bring the U.S. one step closer to subduing the PRC's cyber threats against the U.S. defense supply chain.

Appendix A
PROHIBITION ON USE OR PROCUREMENT.—

(1) The head of an executive agency may not—

(A) procure or obtain or extend or renew a contract to procure or obtain any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system; or

(B) enter into a contract (or extend or renew a contract) with an entity that uses any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system.

(2) Nothing in paragraph (1) shall be construed to—

(A) prohibit the head of an executive agency from procuring with an entity to provide a service that connects to the facilities of a third party, such as backhaul, roaming, or interconnection arrangements; or

(B) cover telecommunications equipment that cannot route or redirect user data traffic or permit visibility into any user data or packets that such equipment transmits or otherwise handles.

(b) PROHIBITION ON LOAN AND GRANT FUNDS.—(1) The head of an executive agency may not obligate or expend loan or grant funds to procure or obtain, extend or renew a contract to procure or obtain, or enter into a contract (or extend or renew a contract) to procure or obtain the equipment, services, or systems described in subsection (a).

Appendix B

—The term “covered telecommunications equipment or services” means any of the following:

- (A) Telecommunications equipment produced by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of such entities).
- (B) For public safety, security of government facilities, physical security surveillance of critical infrastructure, and other national security purposes, video surveillance and telecommunications equipment produced by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of such entities).
- (C) Telecommunications or video surveillance services provided by such entities or using such equipment.
- (D) Telecommunications or video surveillance equipment or services produced or provided by an entity that the Secretary of Defense, in consultation with the Director of the National Intelligence or the Director of the Federal Bureau of Investigation, reasonably believes to be an entity owned or controlled by, or otherwise connected to, the government of a covered foreign country.