Cite as Stewart, 10 J. NAT'L SECURITY L. & POL'Y __ (forthcoming 2019)

Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings

Camille A. Stewart[*]

Bankruptcy is an important part of the U.S. innovation culture.[1] Entrepreneurs that take risks to create cutting edge technology will sometimes fail or exhaust financial resources because the market does not always support the long-term cost of innovation. The opportunity for entrepreneurs to recover a portion of the money invested, absolve themselves of part of the resulting debt, and sell viable technology and intellectual property (IP) to another entity is an essential lifeline that encourages entrepreneurs to continue to take these risks.[2] At the same time, however, the lure of these cutting-edge technologies make bankruptcy proceedings a vehicle for exfiltration of national security-related technology and IP by U.S. adversaries.[3] Left unchecked, this enables nation-states with malicious intent to amass technical capability and insight into military and critical infrastructure systems to support potentially significant cyberattacks.[4]

---

[*] Camille Stewart is an attorney working at the intersection of technology, law, and society. Her crosscutting perspective on complex technology, cyber, national security, and foreign policy issues has landed her in significant roles at leading government and private sector companies like the Department of Homeland Security and Deloitte. Camille is the former Senior Policy Advisor for Cyber, Infrastructure & Resilience Policy at the Department of Homeland Security in the Obama Administration.

This paper was written as part of a program Camille is leading at the Transformative Cyber Innovation Lab (TCIL) at the Foundation for Defense of Democracies to explore sensitive technology leakage through the courts. Visit https://www.camillestewart.com/ or https://www.fdd.org/projects/transformative-cyber-innovation-lab/ for next steps including outcomes of the pilot training for bankruptcy judges.

[1] Daniel Fisher, *The Latest Craze in Silicon Valley: Bankruptcy*, FORBES (Mar. 15, 2017), https://www.forbes.com/sites/danielfisher/2017/03/15/the-latest-craze-in-silicon-valley-bankruptcy/#184362c41664.

[2] *Id.*

[3] National security-related technology and IP cannot be statically defined because of the ever-changing threat landscape and evolving capabilities available and needed to prevail within said landscape. For the purposes of this paper, national security-related technology and IP refers to software, technology, equipment, and intellectual property that must be protected in the best interest of U.S. national security such as dual-use technologies and/or equipment, software, technology, and intellectual property that if tampered with may have detrimental impact on U.S. critical infrastructure and/or the U.S. defense industrial base. This includes anything on the export control lists which are amended, and items added or removed when deemed to no longer warrant control. *E.g.*, Control of Firearms, Guns, Ammunition, and Related Articles, 83 Fed. Reg. 24,166 (May 24, 2018) (to be codified at 15 C.F.R. pts. 736, 740, 741, 743, 744, 746, 748, 758, 762, 772, 774); ''Dual use'' and other types of items subject to the EAR, 15 C.F.R. § 730.3 (2018) ("The term 'dual use' is often used to describe the types of items subject to the EAR. A 'dual-use' item is one that has civil applications as well as terrorism and military or weapons of mass destruction (WMD)-related applications."); Michael Brown & Pavneet Singh, *DIUx Study on China's Technology Transfer Strategy*, DEF. INNOVATION UNIT EXPERIMENTAL 23 (Jan. 2018), https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf; Cory Bennett & Bryan Bender, *How China Acquires 'the Crown Jewels' of U.S. Technology,* POLITICO, (May 22, 2018), https://www.politico.com/story/2018/05/22/china-us-tech-companies-cfius-572413; *Exfiltrate*, MERRIAM-WEBSTER DICTIONARY (2018) (Exfiltration is the unauthorized access to data or information).

[4] DANIEL R. COATS, OFF. OF THE DIR. OF NAT'L INTELLIGENCE, STATEMENT FOR THE RECORD: WORLDWIDE THREAT ASSESSMENT OF THE US INTELLIGENCE COMMUNITY 5-6 (2018),

Nation-states employ a myriad of techniques to make stealth and strategic investments to strengthen the competitive position of their national economies and their militaries.[5] Bankruptcy proceedings have become an opportunity for foreign investors to circumvent the labyrinth of federal regulations designed to prevent foreign investment and technology acquisition that impede U.S. national security.[6] For example, in 2017, Chinese mining company Shenghe Resources acquired the mining rights to the ***sole*** rare earth mine in the United States when Molycorp auctioned off parts of the company as part of bankruptcy proceedings.[7] Rare earth minerals are critical components of many defense and technology products and now other nations control our supply chain for these minerals.

In addition to enhancing their own military capabilities, foreign adversaries can leverage the information acquired to discover and exploit vulnerabilities in the technology to launch highly tailored, sophisticated, and potentially catastrophic cyberattacks and to insert into U.S. supply chains malicious or compromised technology that can be exploited at a later time.[8] The cybersecurity challenge is "no longer an acceptable risk, but an existential threat to the American people's fundamental way of life," according to National Security Telecommunications Advisory Committee report last year.[9] As Assistant Secretary of the Treasury for International Markets and Investment Policy Heath P. Tarbert testified before Congress, "The potential loss of

---

https://www.dni.gov/files/documents/Newsroom/Testimonies/Final-2018-ATA---Unclassified---SASC.pdf; Bennett & Bender, *supra* note 3.

[5] Steve Grobman, *When Nation-States Hack the Private Sector for Intellectual Property*, THE HILL (Mar. 31, 2018), http://thehill.com/opinion/technology/380948-when-nation-states-hack-the-private-sector-for-intellectual-property; *see also* Brown & Singh, *supra* note 3.

[6] Including but not limited to CFIUS, export control regulations - such as Export Administration Regulations and International Traffic in Arms Regulations - and Anti-Assignment Act. *See supra* Part III. Gaps in the Current Legal Framework Preventing Unauthorized Foreign Access to National Security-Related Technology and Intellectual Property.

[7] Johnathan Allen, *Critics Blast $3M Mining Handout*, POLITICO (Oct. 6, 2009), https://www.politico.com/news/stories/1009/27947_Page2.html; Tom Hals, *Rare Earth Miner Molvcorp to Start Bankruptcy Sale of Business*, REUTERS (Jan. 8, 2017), https://www.reuters.com/article/us-bankruptcy-molycorp-idUSKBN0UM2A820160108; John Millner & Anjie Zheng, *Molycorp Files for Bankruptcy Protection*, WALL ST. J. (June 25, 2015), https://www.wsj.com/articles/SB10907564710791284872504581069270334872848; Andrew Topf, *Mountain Pass Sells for $20.5 Million*, MINING (June 16, 2017), http://www.mining.com/mountain-pass-sells-20-5-million/.

[8] DEP'T OF DEF., SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY 3 (2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf; DEP'T OF JUSTICE, REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASKFORCE 47 (2018), https://www.justice.gov/ag/page/file/1076696/download; *CFIUS Reform: Administration Perspectives on the Essential Elements: Hearing Before the S. Comm. on Banking, Housing, & Urban Affairs*, 115th Cong. (2018) (testimony of the Hon. Heath P. Tarbert, Assistant Sec'y of the Treasury).

[9] NAT'L SECURITY TELECOMMS. ADVISORY COMM., NSTAC REPORT TO THE PRESIDENT ON A CYBERSECURITY MOONSHOT (2018), https://www.dhs.gov/sites/default/files/publications/DRAFT_NSTAC_ReportToThePresidentOnACybersecurityMoonshot_508c.pdf.

America's technological and military edge […] will have a real cost in American lives in any conflict."[10]

Recognizing this gap, Congress recently passed legislation that adds transactions that occur "pursuant to a bankruptcy proceeding or other form of default on debt" to the list of transactions over which the Committee on Foreign Investment in the United States (CFIUS) has jurisdiction.[11] CFIUS is an inter-agency committee charged with protecting national security by reviewing economic transactions (such as mergers and acquisitions) involving foreign entities where those foreign entities would gain access to national security-related technology and IP and thereby pose a major threat to U.S national security.[12]

Regulation alone is not enough to combat this threat. Congress's targeted expansion of the legal framework regulating foreign investment is an important but insufficient step toward minimizing leakage of national security-related technology through the court. The judiciary must also be a partner in mitigating the leak. Informed and equipped bankruptcy courts and judges are necessary to promote adherence to the U.S. laws on foreign investment, identify noncompliance with these laws, and protect U.S. national security. Judges already have some tools to intervene in cases before them where national security may be at risk. Through a few strategic changes to bankruptcy forms and, potentially, the law, bankruptcy judges can be further empowered. Tailored training and technical support will equip bankruptcy court judges to more proactively identify and mitigate potential national security concerns raised by the cases on their dockets. While training and support alone will not eradicate the broader challenge of foreign, malign technology acquisition, it can start to stem the current tech hemorrhage by including the judiciary in the solution.

I. Chinese Acquisition of U.S. Technology through Strategic Investment and Bankruptcy

Of Washington's primary adversaries, China's stealth and strategic investment in U.S. national security-related technology and IP is the most robust.[13] Dating back to at least the early

[10] *CFIUS Reform: Administration Perspectives on the Essential Elements*, *supra* note 8.
[11] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 2181 (2018).
[12] *CFIUS Reform: Examining the Essential Elements: Hearing Before the S. Comm. on Banking, Housing, & Urban Affairs*, 115th Cong. (2018) (statement of Chairman Mike Crapo, R-ID); Interview with Giovanna M. Cinelli, Practice Lead of Int'l Trade & Nat'l Security, Morgan, Lewis & Brockius (June 22, 2018); Brown & Singh, *supra* note 3, at 23.
[13] "The main actors are Russia, China, Iran, and North Korea, according to [the U.S. Director of National Intelligence (DNI)] (2017). These groups are well funded and often engage in sophisticated, targeted attacks. Nation-states are typically motivated by political, economic, technical, or military agendas, and they have a range of goals that vary at different times." COUNCIL OF ECON. ADVISERS, THE COST OF MALICIOUS CYBER ACTIVITY TO THE U.S. ECONOMY (2018), https://www.whitehouse.gov/wp-content/uploads/2018/02/The-Cost-of-Malicious-Cyber-

1980s, China has made the acquisition of advanced foreign technology - through means licit and illicit - a centerpiece of its economic development planning and as well as a means to adapt and leverage U.S. technology and knowhow to reduce the U.S. national security advantage.[14] China participates in 10-16 percent of all venture capital deals,[15] and in 2015, Chinese investors participated in deals worth nearly 16 percent of value of all technology deals that year.[16] Leading Chinese cybersecurity firm Qihoo 360 (a company closely linked to the Chinese military and government) founded "a venture capital fund in Silicon Valley in order to support start-ups that it considers strategically significant."[17] The company's founder and CEO Zhou Hongyi also serves as an advisor to an early stage venture capital fund, 11.2 Capital, that "invested in 'breakthrough' technologies, such as artificial intelligence (AI), augmented reality/virtual reality (AR/VR), robotics, and biotechnology, across a range of companies, including Ginkgo Bioworks."[18]

Qihoo 360 is not unique. The Pentagon's Defense Innovation Unit (DIUx) 2018 "Study on China's Technology Transfer Strategy" lists a sampling of Chinese government-back venture firms and their sources of capital.[19] Beijing is strategically backing and investing in efforts to improve its economic and military posture as outlined in plans such as Made in China 2025, "Internet Plus," China's Mega Project Priorities, and President's Xi Jinping's goal to become one of the most innovative economies by 2020.[20] China gains insight into the Silicon Valley ecosystem, emerging technologies, and dual-use and national security-related technology and IP as an early investor. Currently, this avenue is not adequately controlled by CFIUS and other regulations although the changes in the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), if implemented correctly, can close some of this gap.[21]

More to the point, China understands how to circumvent U.S. foreign investment regulations including by pressuring U.S. companies to enter joint ventures, by gaining access to assets through bankruptcy, and by coercing U.S. companies into sharing their capabilities and

---

Activity-to-the-U.S.-Economy.pdf; Coats, *supra* note 4; Bill Gertz, *Report: China's Military Is Growing Super Powerful by Stealing America's Defense Secrets (Like the F-35)*, NAT'L INTEREST (Dec. 8, 2016), https://nationalinterest.org/blog/the-buzz/report-chinas-military-growing-super-powerful-by-stealing-18677.

[14] *CFIUS Reform: Examining the Essential Elements*, *supra* note 12; OFF. OF TECH. ASSESSMENT, OTA-ISC-340, TECHNOLOGY TRANSFER TO CHINA 3 (1987); Ellen Nakashima, *US Said to Be Target of Massive Cyber-Espionage Campaign*, WASH. POST (Feb. 10, 2013), https://www.washingtonpost.com/world/national-security/us-said-to-be-target-of-massive-cyber-espionage-campaign/2013/02/10/7b4687d8-6fc1-11e2-aa58-243de81040ba_story.html.

[15] Brown & Singh, *supra* note 3, at 2.

[16] *Id.* (citing data retrieved from CB Insights, Oct. 2017; data includes all rounds: Seed/Angel, Series A-E+, Convertible Notes, and "Other VC" investments).

[17] *China's Threat to American Government and Private Sector Research and Innovation: Hearing before the H. Permanent Select Comm. on Intelligence*, 115th Cong. (2018) (testimony of Elsa B. Kania, Adjunct Fellow, Ctr. for New Am. Security).

[18] *Id.*

[19] Brown & Singh, *supra* note 3, at app. 4.

[20] *Id.*

[21] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 2181 (2018).

trade secrets. These techniques enable Chinese companies to acquire the accompanying technology, IP, and knowhow and to replicate them.[22] Senator Cornyn further warned, "The Chinese have figured out which dual-use emerging technologies are still in the cradle, so to speak, and not yet subject to export controls."[23]

For example, China acquired Atop Tech in a bankruptcy proceeding in the summer of 2017.[24] Atop Tech produced high-end microchips capable of powering everything from smartphones to high-tech weapons systems. This critical component of the U.S. supply chain is the type of product that would likely be regulated as a dual-use or export-controlled technology as it scaled,[25] but it was not export controlled when the company declared bankruptcy. In the proceeding, Avatar Integrated Systems stepped forward as a buyer. The company's board chairman is a prominent Chinese steel magnate, and his Hong Kong-based company was Avatar's major shareholder.[26] Competitor and creditor, Synopsys, made demands for information citing CFIUS concerns,[27] but Avatar filed a successful motion for protective order barring Synopsys from making requests.[28] The transaction went through without a CFIUS review.[29] This artful maneuvering of the U.S. legal system to circumvent CFIUS review is neither new nor uncommon.[30] This is the kind of case FIRRMA has the potential to prevent, if implemented appropriately.

Strategic ownership of and investment in U.S. technology and IP becomes increasingly concerning when coupled with an adversary's ability to affect the hardware of systems.[31] A 2016 University of Michigan study details how an attacker can leverage analog circuits to create a

[22] *CFIUS Reform: Examining the Essential Elements*, *supra* note 12.
[23] *Id.*
[24] *China's Threat to American Government and Private Sector Research and Innovation*, *supra* note 17.
[25] Bennett & Bender, *supra* note 3.
[26] *China's Threat to American Government and Private Sector Research and Innovation*, *supra* note 17; Bennett & Bender, *supra* note 3.
[27] *In re* Atoptech, Inc., No. 17-10111 (MFW), Motion of Avatar Integrated Systems Inc. for Protective Order, ¶ 1 (Bankr. D. Del. May 8, 2017).
[28] *Id.* at ¶ 5; *In re* Atoptech, Inc., No. 17-10111 (MFW), Order (A) Approving The Asset Purchase Agreement; (B) Approving The Sale To The Purchaser Of Substantially All Of The Assets Of The Debtor Pursuant To Section 363 Of The Bankruptcy Code Free And Clear Of All Liens, Claims, Interests, And Encumbrances; (C) Approving The Assumption And Assignment Of Certain Executory Contracts And Unexpired Leases Pursuant To Section 363 Of The Bankruptcy Code ; (D) Authorizing The Debtors To Consummate Transactions Related To The Above And (E) Granting Other Relief, ¶ 48-49 (Bankr. D. Del. May 22, 2017).
[29] Bennett & Bender, *supra* note 3.
[30] BUREAU OF EXP. ADMIN., OFF. OF STRATEGIC INDUS. AND ECON. SECURITY, U.S. COMMERCIAL TECHNOLOGY TRANSFERS TO THE PEOPLE'S REPUBLIC OF CHINA (1999), https://fas.org/nuke/guide/china/doctrine/dmrr_chinatech.htm.
[31] Andy Greenberg, *This 'Demonically Clever' Backdoor Hides in a Tiny Slick of a Computer Chip*, WIRED (June 1, 2016), https://www.wired.com/2016/06/demonically-clever-backdoor-hides-inside-computer-chip/.

hardware attack that is small, stealthy, and successfully evades known defenses.[32] Nation-state investment in and acquisition of national security-related technology and IP and U.S. cutting-edge technology makers, with products similar to ATopTech, will continue to lead to unknown foreign ownership of critical components of the U.S. supply chain. Imagine a backdoor "invisible not only to the computer's software, but even to the chip's designer, who has no idea that it was added by the chip's manufacturer," a foreign entity working in coordination with their government.[33] The effects of such a supply chain attack could be catastrophic.

II. Exposure During Bankruptcy Proceedings

Even if foreign entities are not a party in the bankruptcy proceeding, there are several points during the process where sensitive company data is exposed to potential buyers, bidders, creditors, and even the general public to varying degrees. Much of the judicial process is public and open, as mandated in the Constitution.[34] U.S. adversaries can learn valuable information in open court even if they do not acquire the assets. When the data has national security implications, the risks from this level of exposure outweigh the desire to have a public trial. Judges have tools to help prevent unnecessary exposure of relevant sensitive information and with some strategic adjustments to rules or the law, judges can be further empowered to reduce exposure.

Companies going through bankruptcy must file schedules of assets and liabilities, a schedule of current income and expenditures, and a statement of financial affairs. Under Chapter 7 and the Chapter 11 petition for bankruptcy, they must also file a schedule of contracts and leases. Each of these documents includes significant amounts of information that is now on file with the court and available to potential buyers[35] and to the public as part of the record unless some protection is put in place.

During the meeting of creditors in a Chapter 7 bankruptcy, participants can ask the debtor questions about their financial affairs and property.[36] In a Chapter 11 bankruptcy, the Creditors' Committee is involved in formulating a plan and investigating the conduct and operation of the business, among other things. These creditor meetings in particular provide a high level of exposure to company proprietary information.[37] Many of these filings and courtroom pleadings

---

[32] Kaiyuan Yang et al., *A2: Analog Malicious Hardware*, UNIV. MICH. DEP'T ELEC. ENG'G & COMP. SCI, 1, http://static1.1.sqspcdn.com/static/f/543048/26931843/1464016046717/A2_SP_2016.pdf?token=N4pJSSoqL4kE4V4JXpTwx7qDRX4%3D.
[33] Greenberg, *supra* note 31.
[34] U.S. CONST., amend. VI ("In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury […]").
[35] FED. R. BANKR. P. 1007(b).
[36] 11 U.S.C. § 343 (2012); 11 U.S.C. § 341(c) (2012).
[37] 11 U.S.C. § 1102 (2005).

are viewed by courtroom observers and accessible upon request by almost anyone else.[38] Additionally, prior to purchasing the company, parties may also review national security-related technology and IP during the Chapter 7 sale of property by a trustee as long as the property is not exempt per local regulations.[39] Patents, tech schematics, trade secrets, and other proprietary information may be included.

Although bankruptcy court judges have limited visibility into the interactions and negotiations leading up to a plan or bid, during the course of a proceeding, judges can protect sensitive corporate information that may have national security implications.[40] Confidentiality, such as submitting information as confidential business information and requesting protective orders, is "an ever-expanding feature of modern litigation" that is useful in cases where counsel is concerned about exposing sensitive corporate information.[41] Additionally, a judge can review evidence or conduct a hearing in his/her private chambers away from the jury or public eye using what is known as "in camera review."[42] This can prevent some of the exposure of sensitive data in open court. Although requests for in camera review are often made by counsel for the parties, the judge can do so *sua sponte* (of his or her own accord) for whatever reason including if the judge suspects there are national security implications.

Changes to bankruptcy court rules and the law can also grant enhanced visibility to identify potential national security implications in cases and/or protect sensitive information during proceedings. The creation of a secrecy order, similar to but less imposing than the secrecy orders under the Invention Secrecy Act, would place confidentiality restrictions on national security-related technology and IP during trial.[43]

III. Gaps in the Current Legal Framework Preventing Unauthorized Foreign Access to National Security-Related Technology and Intellectual Property

[38] *Obtaining Copies of Court Records in the Federal Records Centers*, NAT'L ARCHIVES, https://www.archives.gov/research/court-records/bankruptcy.html.
[39] 11 U.S.C. § 721 (2011) ("Any nonexempt property—property owned by the debtor that exceeds the amount allowed by the state—is sold by the trustee to pay creditors").
[40] 11 U.S.C. § 341(c) (prohibiting judges from attending meetings with creditors and equity security holders).
[41] *In re* Mirapex Prods. Litig., 246 F.R.D. 668, 672–73 (D. Minn. 2007).
[42] *In camera (legal)*, WEST'S ENCYCLOPEDIA OF AM. L. (2d ed. 2008).
[43] The secrecy orders, issued under the Invention Secrecy Act of 1951, restrict disclosure of patent applications considered to be "detrimental to national security" if published. U.S. PATENT & TRADEMARK OFFICE, MANUAL OF PATENT EXAMINING PROCEDURE: REVIEW OF APPLICATIONS FOR NATIONAL SECURITY AND PROPERTY RIGHTS ISSUES (2015). When a patent application is screened by the USPTO, if it might impact national security, it is referred to the appropriate agencies for consideration of restrictions on disclosure. *Id.* Most invention secrecy applies to inventions involving technology relevant to military applications, but the full scope of the invention secrecy program is not described in public documents. *Id.*

CFIUS, the U.S. export control regime, and regulations over government contracts are the legal framework designed to prevent hostile foreign access to national security-related technology and IP.[44] Yet, they are insufficient because their jurisdiction and enforcement are limited and the threat is ever evolving.[45] Moreover, much of the reporting and classification in these regulations is voluntary or otherwise left to the entity itself to navigate, causing errors that expose restricted information. Export control authorities do not proactively "seek out companies developing new technologies" or "investigate the relationship between investors and employees of a startup."[46]

A. Committee on Foreign Investment in the United States (CFIUS)

CFIUS is one of the main tools to prevent foreign investment in the U.S. that poses a national security threat. Codified by the Foreign Investment and National Security Act of 2007,[47] the committee traditionally only reviewed transactions that resulted in a foreign controlling interest.[48] As a result, minority investments, sliding scale investments, and other investment models were unregulated.[49] Recognizing these and other gaps in CFIUS regulations, Congress passed FIRRMA as part of the National Defense Authorization Act for Fiscal Year 2019.[50] The legislation expands the list of covered sectors of the economy to include technologies critical to U.S. national security but not controlled under any other export control provisions[51] and expands the scope of covered transactions by, *inter alia*, codifying that CFIUS has jurisdiction over transactions that occur "pursuant to a bankruptcy proceeding or other form of default on debt"[52] and over any "transaction, transfer, agreement, or arrangement […] which is designed or intended to evade or circumvent" CFIUS review.[53]

The U.S. Treasury Department issued its first set of pilot program regulations on October 10, 2018 (in effect as of November 10, 2018) to begin to implement FIRRMA.[54] The pilot program identifies 27 critical industries, defined by NAICS (North American Industry

[44] *CFIUS Reform: Examining the Essential Elements*, *supra* note 12; Cinelli, *supra* note 12.
[45] Brown & Singh, *supra* note 3, at 2, 23.
[46] Brown & Singh, *supra* note 3, at 23.
[47] Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246 (2007).
[48] *CFIUS Reform: Examining the Essential Elements*, *supra* note 12; Brown & Singh, *supra* note 3, at 2, 23.
[49] *Id.*
[50] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 2177-83 (2018).
[51] Stephanie Zable, *The Foreign Investment Risk Review Modernization Act of 2018*, LAWFARE BLOG (Aug. 2, 2018, 3:39 PM), https://www.lawfareblog.com/foreign-investment-risk-review-modernization-act-2018.
[52] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 2181 (2018).
[53] Foreign Investment Risk Review Modernization Act of 2018, H.R. 5841, 115th Cong. § 1703(a)(4) (2018).
[54] Pilot Program to Review Certain Transactions Involving Foreign Persons and Critical Technologies, 31 C.F.R. pt. 801 (2018).

Classification System) codes.[55] According to the U.S. Department of Treasury, these are "industries for which certain strategically motivated foreign investment could pose a threat to U.S. technological superiority and national security."[56]

Under these new regulations, parties in bankruptcy proceedings are required to submit for CFIUS review if there is the acquisition of an equity interest that affords a foreign person access to specified information or governance rights.[57] However, in bankruptcy proceedings, there are currently limited parties-in-interest[58] that can be counted on to demand a CFIUS application or recognize a potential national security concern.[59] Debtors and their foreign investor or purchaser are focused on closing the deal.[60] Creditors' desire to obtain the highest recovery in a timely and cost-efficient manner often runs counter to seeking review.[61] One of the few parties that may benefit from a CFIUS review is a losing U.S. bidder, and such a bidder would likely lack standing to seek review.[62] Protective orders and other filings can also limit CFIUS-related inquiries or requests for review.[63]

A lack of routine enforcement for failures to file with CFIUS also means that companies are less concerned that an approved transaction will be unwound for failure to initiate a CFIUS application.[64] There is no formal process for identifying transactions that should have undergone CFIUS review after the fact,[65] and even so, a CFIUS review after a company has been acquired – even if the acquisition is reversed – may be too late. The foreign entity may have already accessed all the national security-related technology and IP as a party to the proceeding. The

---

[55] *North American Industry Classification System*, U.S. CENSUS BUREAU (2017), https://www.census.gov/eos/www/naics/ ("The North American Industry Classification System (NAICS) is the standard used by Federal statistical agencies in classifying business establishments for the purpose of collecting, analyzing, and publishing statistical data related to the U.S. business economy.").
[56] *Fact Sheet: Interim Regulations for FIRRMA Pilot Program*, U.S. DEP'T OF TREASURY (Oct. 10, 2018), https://home.treasury.gov/system/files/206/Fact-Sheet-FIRRMA-Pilot-Program.pdf.
[57] Pilot Program to Review Certain Transactions Involving Foreign Persons and Critical Technologies, 31 C.F.R. pt. 801 (2018).
[58] *Party in Interest*, THOMSON REUTERS PRAC. L. GLOSSARY (2019) ("Bankruptcy, a party to a matter in a bankruptcy case with standing to be heard in court. In most bankruptcy cases, parties in interest include the debtor, creditors and US Trustee.").
[59] Richard A. Chesley & Daniel Simon, *The Intersection of National Security and Bankruptcy*, LAW360 (Apr. 8, 2013, 10:58 AM), https://www.law360.com/articles/430781/the-intersection-of-national-security-and-bankruptcy.
[60] *Id.*
[61] *Id.*
[62] *Id.*
[63] *See, e.g.*, *In re* Atoptech, Inc., No. 17-10111 (MFW), Motion of Avatar Integrated Systems Inc. for Protective Order, ¶ 1 (Bankr. D. Del. May 8, 2017) (A bidder for bankrupt microchip design software company, ATopTech, Inc, operating in an industry that has become the focus of heightened national security attention, sought a protective order barring a Chapter 11 creditor from making several information demands).
[64] Chesley & Simon, *supra* note 59.
[65] Bennett & Bender, *supra* note 3.

good news is that because NAICS codes are often provided in bankruptcy filings,[66] judges can identify cases where CFIUS has jurisdiction and require noncompliant parties to submit to a CFIUS review.[67]

Treasury has not yet issued regulations to expand on FIRRMA's inclusion of bankruptcies and other debt proceedings under CFIUS jurisdiction.[68] The most efficient way to incorporate bankruptcy and other debt proceedings into the CFIUS review process is explicitly adding them to the existing short-form declaration process.[69] At the very least, bankruptcy and other proceedings need to be clearly addressed in CFIUS FAQs.

Judicial vigilance and the threat of U.S. federal government review may cause foreign buyers with malicious intent to withdraw their bids.[70] For example, telecommunications company, Global Crossing, proposed to exit bankruptcy by selling itself to two foreign purchasers including a Hong-Kong based firm.[71] The bankruptcy court noted that the connection of this company to the Chinese government "plainly made securing approval from CFIUS [...] difficult or impossible."[72] As a result of the specter of CFIUS involvement, the Hong Kong company withdrew its portion of the bid.[73]

Unfortunately, even with the inclusion of bankruptcies and other debts as covered transactions, gaps remain in CFIUS jurisdiction as it relates to bankruptcy proceedings. For example, A123 Systems developed a new process for fast-charging lithium-ion batteries.[74] While the new technology appeared promising and despite receiving significant government funds, the combination of a nascent battery industry, the 2008 recession, and a large battery recall proved insurmountable.[75] In an effort to stay in business, A123 Systems announced a plan to sell an 80

---

[66] Pilot Program to Review Certain Transactions Involving Foreign Persons and Critical Technologies, 31 C.F.R. pt. 801 (2018).
[67] U.S. DEP'T OF TREASURY, *supra* note 56.
[68] John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. No. 115-232, 132 Stat. 1636, 2181 (2018).
[69] Provisions for a Pilot Program to Review Transactions Involving Foreign Persons and Critical Technologies, 83 Fed. Reg. 51,322.
[70] Anthony Michael Sabino, *The Upcoming Role of CFIUS in the Westinghouse Bankruptcy*, N.Y. L.J. (May 24, 2017, 2:01 PM), https://www.law.com/newyorklawjournal/almID/1202787342937/the-upcoming-role-of-cfius-in-the-westinghouse-bankruptcy/.
[71] *Id.* (citing *In re* Global Crossing Ltd., 295 B.R 726 (Bankr. S.D.N.Y. 2003)).
[72] *Id.*
[73] *Id.*
[74] Brad Plumer, *A123 Systems Files for Bankruptcy: Here's What You Need to Know*, WASH. POST (Oct. 16, 2012), https://www.washingtonpost.com/news/wonk/wp/2012/10/16/a123-systems-files-for-bankruptcy-heres-what-you-need-to-know/?utm_term=.9f05ef7e3b60.
[75] Tom Hals & Ben Klayman, *Chinese Firm Wins A123 Despite U.S. Tech Transfer Fears*, REUTERS (Jan. 29, 2013, 8:50 AM), https://www.reuters.com/article/us-a123-wanxiang-approval/chinese-firm-wins-a123-despite-u-s-tech-transfer-fears-idUSBRE90S0JN20130129; Plumer, *supra* note 74.

percent stake to Chinese auto-parts maker Wanxiang Group Corporation for $465 million.[76] Wanxiang backed out of the deal after members of Congress voiced concerns about the company being sold to a Chinese firm and after it became clear the deal would necessitate filing for CFIUS review.[77] Unable to recover, an outcome Wanxiang likely anticipated, A123 Systems filed for bankruptcy protection under Chapter 11.[78] Wanxiang purchased the assets at a bankruptcy auction, prevailing over a U.S. bidder.[79] CFIUS approved the deal in January 2013.[80] Experts speculate that Wanxiang knew the company would have a better chance of success if the sale resulted from bankruptcy.[81] If CFIUS reviews triggered by bankruptcy are reviewed with less rigor, the updates to CFIUS regulation will have failed to address the problem.

B. Export Controls

The United States export control regulatory regime is designed to restrict and manage the sale of sensitive equipment, software and technology to foreign persons in accordance with U.S. national security interests and foreign policy objectives.[82] The Commerce Department's Bureau of Industry and Security (BIS) administers the Export Administration Regulations which govern dual-use[83] and certain military items. The State Department's Directorate of Defense Trade Controls administers the International Traffic in Arms Regulations, which govern "defense articles" and "defense services."[84] The third major export control regulation is the International Emergency Economic Powers Act which authorizes the president to block transactions and freeze assets when there is an unusual and extraordinary threat to U.S. national security.[85] Sanctions programs like those against Iran and North Korea fall under this third set of regulations. Failure to strictly adhere to any of these laws and regulations can result in severe consequences ranging from fines to suspension of a company's U.S. export privileges to jail time

[76] Patrick Fitzgerald et al., *Battery Maker Files for Bankruptcy*, WALL ST. J. (Oct. 16, 2012, 7:59 PM), https://www.wsj.com/articles/SB10000872396390443854204578060433271656440.
[77] Ramsey Cox, *Grassley, Thune Demand Answers on Whether Stimulus Dollars Benefited China*, THE HILL (Oct. 12, 2018, 1:08 PM), https://thehill.com/blogs/floor-action/senate/261675-grassley-thune-demand-answers-on-whether-stimulus-dollars-benefited-china-.
[78] Plumer, *supra* note 74.
[79] Charles Ridley, *China's Wanxiang Wins Auction for A123*, CNN MONEY (Dec. 10, 2012, 9:18 AM), https://money.cnn.com/2012/12/10/news/wanxiang-a123-auction/index.html.
[80] Hals & Klayman, *supra* note 75.
[81] Not-for-attribution, confidential expert roundtable interview, *Foundation for Defense of Democracies* (Oct. 15, 2018).
[82] *Overview of U.S. Export Control System*, U.S. DEP'T OF STATE, https://2009-2017.state.gov/strategictrade/overview/index.htm.
[83] 15 C.F.R. § 730.3 (2018).
[84] Export Administration Regulations, 15 C.F.R. pts. 730-74 (2019); International Traffic in Arms Regulations, 22 C.F.R. pts. 120-30 (2019).
[85] Allan Goldner, Lianzhong Pan & Johnathan Todd, *The ZTE Case: U.S. Sanctions and Export Control Laws*, BENESCH (May 5, 2017), https://www.beneschlaw.com/The-ZTE-Case-US-Sanctions-and-Export-Control-Laws-05-05-2017/.

for individuals who willfully violate the law.[86] In general, export controls prevent specific exports to specific countries but are not well-designed "to govern early-stage technologies or investment activity," according to a DIUx study.[87]

While companies can ask relevant government agencies to classify products for them, or support an export classification determination,[88] exporters are permitted to self-classify their products - i.e., determine on their own the proper export classification of their products.[89] As a result, technology that should be controlled may be misclassified or incorrectly determined out of scope and sold to foreign entities where a sale may have otherwise been prohibited.[90]

While bankruptcy court judges have limited visibility into the interactions and negotiations leading up to a plan or bid,[91] if they are knowledgeable about national security and export controls, they can use export control regulations to intervene and mitigate potential harm.[92] Judges can require cases to undergo CFIUS review, request proof of CFIUS review, and identify cases for review under export controls. Most importantly, if they are trained in national security and export control regulations, judges can also deny sales or order changes or modifications to the plan or purchase agreement in the interest of national security.[93]

C. Anti-Assignment Act

The Anti-Assignment Act provides that "[t]he party to whom the Federal Government gives a contract or order may not transfer the contract or order, or any interest in the contract or order, to another party."[94] This prohibition prevents the transfer of government contracts except through the process of novation, the substitution of a new contract in place of the existing.[95] As a

[86] *Overview of U.S. Export Control System*, U.S. DEP'T OF STATE, https://2009-2017.state.gov/strategictrade/overview/index.htm.
[87] Brown & Singh, *supra* note 3, at 2.
[88] Eric Carlson & Peter Lichtenbaum, *China-Related Export Control Risks*, COVINGTON & BURLING LLP, https://www.cov.com/-/media/files/corporate/publications/2016/01/china_related_export_control_risks_january_2016.pdf.
[89] *Id.*
[90] "In June 2012, United Technologies Corp. ("UTC") and its subsidiaries acknowledged that they had failed to properly establish the jurisdiction of defense articles and technical data exported to China to support the design and development of a military attack helicopter. Specifically, a UTC U.S. subsidiary supplied software to operate an engine control system for engines which were ultimately used in the Chinese military helicopters prototypes, but UTC entities failed to recognize that the modification subjected the software to ITAR controls." Carlson & Lichtenbaum, *supra* note 88 (citing U.S. DEP'T OF STATE, BUREAU OF POLITICAL-MILITARY AFFAIRS, CONSENT AGREEMENT IN THE MATTER OF UNITED TECHNOLOGIES ¶¶ 27-29 (June 19, 2012)).
[91] 11 U.S.C. § 341(c) (prohibiting judges from attending meetings with creditors and equity security holders).
[92] Interview with Nova Daly, Senior Public Policy Advisor, WileyRein (July 24, 2018).
[93] FED. R. BANKR. P. 3017.
[94] 41 U.S.C. § 6305(a) (2012).
[95] *Novation,* MERRIAM -WEBSTER DICTIONARY (2018) (Novation is "the substitution by mutual agreement of one obligation for another with or without a change of parties and with the intent to extinguish the old obligation."); *see,*

result, no government contract can be sold to foreign entities.[96] However, start-ups now contribute in whole or in part to many dual-use or military technologies, which means that anti-assignment clauses may need to be included in a broader range of agreements such as contracts with start-ups through DIUx and agreements federal vendors have throughout their supply chain. All departments and agencies should consider requiring anti-assignment or modified anti-assignment clauses throughout their supply chain. Anti-assignment clauses can further empower judges to identify client portfolios with links to the federal supply chain and by providing judges the explicit authority to require novation for contracts in the federal supply chain which may have national security implications.

IV. Training and Equipping Bankruptcy Judges to Identify Potential National Security Concerns

While changes to the regulations are an important component of addressing the gaps and vulnerabilities in the current legal regime, an informed and proactive judiciary is a necessary complement. Judges are a last line of defense in preventing exfiltration of sensitive technology.

Bankruptcy judges and attorneys representing the parties in a bankruptcy case may be best suited to identify potential national security concerns related to foreign investment and export controls prior to significant exposure.[97] Training will not turn judges and attorneys into national security experts. However, training can elevate the issue for judges and provide enough background that they can ask questions to begin to determine the sensitivity of a technology.[98] With training, judges will know to request proof of necessary review (e.g., CFIUS, export control) and will understand who to contact for context. Training can also encourage collaboration and information sharing among judges to identify additional avenues to address the threat and request changes to filing processes and forms.[99]

---

e.g., *Thompson v. Comm'r of Internal Revenue*, 205 F.2d 73, 76 (3d Cir. 1953); *see also* 48 C.F.R. § 42.1204(b) (2014) (providing that novation agreements, pursuant to which the Government consents to a transfer of contracts, are not necessary for a change of ownership as a result of a stock purchase).

[96] Richard Lieberman, *Can You Sell a Government Contract: Assignment, Novation, Change of Name and Assignment of Claims*, PUB. CONTRACTING INST. (May 6, 2016), http://publiccontractinginstitute.com/can-you-sell-a-government-contract-assignment-novation-change-of-name-and-assignment-of-claims/.

[97] MODEL RULES OF PROF'L CONDUCT r. 1.3 cmt. (AM. BAR ASS'N 2019). Attorneys are obligated to advocate for the best interest of their client, and their focus, therefore, may not be in the national security interest. *See id.* However, these attorneys are the pipeline for future bankruptcy judges, and thus it is important to engage the broader legal community to elevating these national security concerns for current and future judges. *See id.*

[98] *See* 28 U.S.C. § 620 (2018) (establishing the Federal Judicial Center which allows judges to play a role in the development and/or execution of specialty course offerings and to work with experts, educational advisory committees, and the board of advisors for the FJC to identify and address knowledge gaps among all federal judges).

[99] James C. Duff, *Overview for the Bench, Bar, and Public*, ADMIN. OFFICE OF THE U.S. COURTS, https://www.uscourts.gov/rules-policies/about-rulemaking-process/how-rulemaking-process-works/overview-bench-bar-and-public ("Proposed changes in the rules are suggested by judges, clerks of court, lawyers, professors, government agencies, or other individuals and organizations.").

Continuing education is, however, largely, if not entirely, voluntary for bankruptcy judges. Bankruptcy judges do not have training requirements as a condition of their position, and states often waive judges' Continuing Legal Education (CLE) requirements while they are on the bench.[100] And yet, bankruptcy and legal communities have begun to express an interest in better understanding national security threats.[101] Discussions of the exfiltration of national security-related technology and IP from bankruptcy courts in the media, in industry publications and forums, and in scholarly works will elevate the issue and promote a recognition that changes are necessary to better address these challenges.[102]

Curated content from knowledgeable experts that educates and empowers judges and attorneys can also facilitate collaboration across branches of government to mitigate national security threats more effectively. The plan implemented to alleviate CFIUS concerns in the ongoing Takata bankruptcy illustrates the importance of understanding the threat and communication and collaboration between the judiciary and the executive branch. Japan-based Takata Corporation is one of the largest manufacturers of automotive parts in the world. On June 25, 2017, TK Holdings, the U.S. operations section of Takata Corporation, filed for Chapter 11 bankruptcy.[103] The bankruptcy announcement came after an airbag crisis linked to at least 16 deaths and several hundred injuries.[104] Members of Congress and experts raised CFIUS concerns because of a proposed sale to rival company Key Safety Systems, a Michigan-based company owned by China's Ningbo Joyson Electronic Corporation. The bankruptcy court, the parties, and CFIUS developed a plan to resolve all objections to the proposed reorganization.[105] Understanding the threat at a high-level and knowing what entity to engage underpinned this resolution. The understanding and resources gained from training can facilitate appropriate collaboration between the judiciary and the executive branch to reduce the time it takes to start this kind of mitigation and more to the point, equip judges to identify the potential need for executive review in line with regulatory requirements.

---

[100] HAW. STATE BAR ASS'N, *Mandatory Continuing Legal Education*, https://hsba.org/HSBA/MCLE/Mandatory_Continuing_Legal_Education.aspx (waiving CLE requirements for Judges in Hawaii).

[101] Not-for-attribution, confidential expert roundtable interview, *Foundation for Defense of Democracies* (Oct. 15, 2018).

[102] Richard H. Thaler & Cass R. Sunstein, NUDGE: IMPROVING DECISIONS ABOUT HEALTH, WEALTH, AND HAPPINESS, PGS 6-8, (2008). This messaging can serve as a "nudge" to promote a choice environment where judges see the importance of the issue and choose to support it. *See id.*

[103] *In re* TK Holdings, Inc., No. 17-11375, Voluntary Petition for Non-Individuals Filing for Bankruptcy (Bankr. D. Del. June 25, 2017).

[104] Jethro Mullen, *Takata, Brought Down by Airbag Crisis, Files for Bankruptcy*, CNN BUS. (June 26, 2017, 11:23 AM), https://money.cnn.com/2017/06/25/news/companies/takata-bankruptcy/index.html.

[105] Tom Hals, *Takata Has Resolved Most Objections to its U.S. Bankruptcy: Lawyer*, REUTERS (Feb. 16, 2018, 12:25 PM), https://www.reuters.com/article/us-takata-bankruptcy-hearing/takata-has-resolved-most-objections-to-its-u-s-bankruptcy-lawyer-idUSKCN1G01YT.

This kind of collaboration may bring up questions of judicial deference to executive statutory interpretation.[106] Bankruptcy judges, however, currently require proof of CFIUS, export control, anti-assignment, and other relevant reviews prior to proceeding on bankruptcy cases with overt national security linkages. This paper does not seek to debate the validity or relevance of judicial deference,[107] rather it argues that bankruptcy judges ought to require that same proof for cases where the national security nexus may not be as overt or may not yet be codified. Better understanding of the threat and clear points of contact between bankruptcy judges and the executive branch will facilitate quicker adaptation to the changing law and threat landscape. Additionally, to the extent that judicial deference becomes a question, training will provide resources for judges to make necessary determinations without relying solely on the advice of their executive branch colleagues.

Technology can also support judicial awareness and identification of sensitive technologies that may be national security-related technology and IP moving through their courts. Commerce Department's BIS is leading an interagency effort to define and determine criteria for identifying emerging technologies that are essential to U.S. national security but have not yet been added to export control or other sensitive technology lists.[108] A database that leverages machine learning to automate comparing the technology at issue in a case with the criteria for "emerging technology" as determined by the BIS effort or other relevant data points like NAICS codes to determine technologies that may warrant review would be valuable to the executive and legislative branches alike.[109] Court filings contain data that if correlated could provide early warnings of sensitive, early-stage technology whose sale to foreign persons may pose a concern. This technological solution could facilitate rapid review of dense data related to past cases and the technology at issue. Bankruptcy judges can then leverage that information to require a review or otherwise take action under the law.

V. Conclusion

Training and education are an essential next step to empowering bankruptcy court judges to be active participants in mitigating the exfiltration of national security-related technology and IP from the court. Without an informed and empowered judiciary to support the efforts of the executive and legislative branches, exfiltration will persist. Nation states will continue to capitalize on this loophole, adapting their techniques to fit the legislative framework.

---

[106] Antonin Scalia, *Judicial Deference to Administrative Interpretations of Law*, 1989 DUKE L.J. 511, 514-16 (1989).
[107] Aditya Bamzai, *The Origins of Judicial Deference to Executive Interpretation*, 126 YALE L.J. 908, 1000-01 (2017).
[108] Review of Controls for Certain Emerging Technologies, 83 Fed. Reg. 58,201 (proposed Nov. 19, 2018) (to be codified at 15 C.F.R. pt. 744).
[109] *Id*.

After judges are trained, they will need resources and support to efficiently and effectively identify and mitigate the exfiltration of national security-related technology and IP from their cases. Training will be more impactful if it is coupled with connections to appropriate executive branch contacts, reference materials, and technology to automate detection of and, eventually, anticipate emerging sensitive technology. Sustained financial, intellectual, and political resource investment in mitigating exfiltration of national security-related technology and IP is necessary to protect the U.S. from losing its military advantage in this ever-changing threat environment.