

Advisory Committee on Rules of Bankruptcy Procedure

# Comments Related to U.S. Bankruptcy Court Rules and their Impact on U.S. National Security

CAMILLE STEWART, ESQ.

**Program Lead**

*Transformative Cyber Innovation Lab  
Foundation for Defense of Democracies*

GIOVANNA M. CINELLI, ESQ.

**Partner and Practice Lead, International Trade & National Security**

*Morgan Lewis & Bockius LLP*

**Board of Advisors**

*Center on Cyber and Technology Innovation  
Foundation for Defense of Democracies*

Washington, DC  
January 30, 2020

Thank you for the opportunity to provide comments concerning the potential impact of the Bankruptcy Court's rules on U.S. national security interests. Although federal court rules generally consider national security when deciding matters related to classified or certain proprietary and law enforcement related information, the rules have tended not to consider that the public nature of court proceedings might require special procedures to protect export-controlled and dual-use information with national security implications. The following comments focus on areas where refinements to the court's rules – through management of the court process, whether docketing, submission management, or courtroom engagement – may assist in protecting broader U.S. national interests. These comments are submitted for the Committee's consideration by Camille Stewart<sup>1</sup> and Giovanna M. Cinelli.<sup>2</sup>

## BACKGROUND

The U.S. federal court system is predicated on public access to the matters being adjudicated by the courts. This open access provides the public with an understanding of how the court system functions, the cases and parties submitting disputes for resolutions, and insight into potential interpretations of complex U.S. laws and regulations. Open access, therefore, serves a strong public purpose.

This access, however, is also susceptible to misuse or exploitation by foreign nation states and state-backed enterprises. From a national security perspective, this is particularly concerning where the matters under review include detailed technical information about products, services, or technology. Court cases involving bankruptcy – in particular, bankruptcy proceedings related to high technology companies – provide a window into the assets these companies possess, both at a financial and technological level. Left unaddressed, this exploitation enables parties with other than solely commercial intentions to access and obtain detailed technical capability as well as

---

<sup>1</sup> **Ms. Camille Stewart** currently serves as a program lead for the Foundation for Defense of Democracies' Transformative Cyber Innovation Lab. She is the author of the report, [Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings](#). Ms. Stewart is an attorney whose crosscutting perspective on complex technology, cyber, and 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. In the Obama administration, Ms. Stewart served as the Senior Policy Advisor for Cyber Infrastructure & Resilience Policy at the Department of Homeland Security. Ms. Stewart is also a New America Cyber Policy Fellow, Truman National Security Fellow, and Council on Foreign Relations Term Member.

<sup>2</sup> **Ms. Giovanna M. Cinelli** is the leader of the International Trade and National Security practice at Morgan Lewis & Bockius LLP and a National Security Fellow at the George Mason University National Security Institute. She is also a member of the Board of Advisors of the Center on Cyber and Technology Innovation at the Foundation for Defense of Democracies. For more than 30 years, she has counseled clients in the defense and high-technology sectors on a broad range of issues affecting national security and export controls, including complex export/import compliance matters, CFIUS and cross-border due diligence, and export enforcement, both classified and unclassified. She handles complex civil and criminal export/import-related investigations and advises on transactional due diligence for regulatory requirements involving government contracts, foreign direct investment, export policy, and compliance. She has testified before Congress on CFIUS legislation and has been a member of several federal advisory committees at the Departments of State, Defense and Commerce. In addition to her legal career, Ms. Cinelli had the privilege of serving in the United States Navy as a Special Duty Intelligence Officer specializing in former Soviet and Russian platforms and industrial base matters.

insight into military and critical technology and infrastructure systems. This information can be used for a variety of purposes, including to support potentially highly damaging cyberattacks.

The problem of unregulated access to technology has been explored outside the bankruptcy context by the Government Accountability Office, the Department of Defense, the Defense Innovation Unit, The MITRE Corporation, and the Congressional Research Service. The impact of this unregulated access in the bankruptcy process and the need for remediation have been explored in a recently published article by Ms. Stewart, *“Full Court Press: Preventing Foreign Adversaries from Exfiltrating National Security Technologies Through Bankruptcy Proceedings.”*<sup>3</sup>

The U.S. executive branch utilizes a number of legal and regulatory tools to monitor and manage access to sensitive and dual-use goods and technology. These tools include the Committee on Foreign Investment in the United States (“CFIUS” or “the Committee”) and U.S. export laws.

Two primary export control regimes, outside of agriculture, govern transfers of products, services and technology from the United States to foreign persons (wherever located): 1) the Export Administration Regulations (“EAR”), 15 CFR parts 730-774, which control the permanent export, release, reexport or retransfer of items (including products, services, software, materials and technology) subject to the EAR (whether included on the Commerce Control List or not)(generally referred to as dual-use items); and 2) the International Traffic in Arms Regulations (“ITAR”), 22 CFR parts 120-130, which control the permanent and temporary export of defense articles, defense services, and related technical data (included on the U.S. Munitions List). These regulations establish a licensing, recordkeeping, reporting and enforcement framework designed to address U.S. national security and foreign policy interests.

CFIUS, meanwhile, analyzes the national security implications of foreign direct investment in the United States, and the export laws seek to manage the transfer of goods, services and technology to foreign parties, whether located in the U.S. or abroad. While CFIUS reviews cross-border investments in the United States, which include mergers, acquisitions, and certain investments of less than full ownership or control, the Committee does not routinely review investments made by foreign parties through the purchase of assets or businesses in the bankruptcy process. This is not because CFIUS lacks jurisdiction to review these transactions, but because the nature of the proceedings does not readily inform the courts of when such review is necessary or, in some instances, required. Although CFIUS has reviewed some bankruptcy related proceedings in the past,<sup>4</sup> CFIUS lacks consistent and cogent visibility within the U.S. court system. This gap has created the opportunity for exploitation.

Congress believed that such reviews were sufficiently critical that it included an express provision in the recent CFIUS reform legislation, the Foreign Investment Risk Review Modernization Act of 2018 (“FIRRMA”). Section 1703(a)(4)(F) states that covered transactions include bankruptcy proceedings. This language recognizes the need to close the gap regarding the potential misuse of

---

<sup>3</sup> Stewart, 10 NAT’L SECURITY L. & POL’Y \_\_ (forthcoming 2019) ([http://jnslp.com/wp-content/uploads/2019/09/Full\\_Court\\_Press\\_Stewart.pdf](http://jnslp.com/wp-content/uploads/2019/09/Full_Court_Press_Stewart.pdf))

<sup>4</sup> See, e.g., E. Wesoff. “A123 Goes to Wanxiang in \$260M Bankruptcy Auction Bid,” *GreenTech* (December 9, 2012); “US Approves A123 Sale to Chinese Firm Despite Security Concerns,” Fox News (January 29, 2013).

the bankruptcy system to obtain technology or technical information that may not otherwise be available to foreign purchasers or investors.

Despite the recent reform, U.S. adversaries (and sometimes competitors) continue to circumvent executive branch processes by purchasing interests in companies in bankruptcy and by leveraging bankruptcy proceedings to obtain access to sensitive technology and intellectual property (IP). This circumvention can pose a threat to U.S. national security, not only as a backdoor to assets that may not otherwise be available if the requests for access were adjudicated by CFIUS or under U.S. export laws, but as a process that can directly or indirectly affect the U.S. industrial base. A one-branch strategy, however, relying only on existing export and investment regulations will limit the nation's ability to prevent or address the misuse of critical information.

Instead, the judicial branch has a critical role to play. The Bankruptcy Court manages its proceedings through rules that provide a framework for the protection of some sensitive information. This existing framework provides the court with certain tools that may be enhanced to address the protection of technical information during the proceeding and may also be used to ensure the relevant transactions receive CFIUS review. These tools can also help limit the circumvention of the export licensing process. In that context, we suggest three tailored enhancements to streamline the identification and protection of relevant technologies prior to their transfer to a foreign party.

The Bankruptcy Court's timely review of its rules provides the opportunity to share some perspective of where and how the court rules may aid in the prevention of exploitation of the court system and concomitant protection of national security interests. We look forward to responding to any questions you may have.

## RECOMMENDATIONS

**1. To help judges identify sensitive or critical technology with potential national security implications, require North American Industry Classification System ("NAICS") codes<sup>5</sup> and export classifications for each technology at issue in a case.**

As part of the Executive Branch's implementation of FIRRMA, the U.S. Treasury Department issued new "pilot program" regulations on October 10, 2018.<sup>6</sup> The pilot program mandates CFIUS filings for all transactions involving foreign persons in 27 critical industries, defined by NAICS

---

<sup>5</sup> Court Alert – New CFIUS Regulations Implement Mandatory Filings Prior to Foreign Ownership – NAICS Codes Implications, issue November 2018. (<https://www.camillestewart.com/s/Court-Alert-New-CFIUS-Regulations-by-Camille-Stewart.pdf>)

<sup>6</sup> Giovanna M. Cinelli, Kenneth J. Nunnenkamp, Stephen Paul Mahinka, Carl A. Valenstein, "CFIUS Scratches the FIRRMA Itch – Pilot Programs Begin Early Implementation," *Morgan, Lewis & Bockius LLP*, October 11, 2018. (<https://www.morganlewis.com/pubs/cfius-scratches-the-firma-itch-pilot-programs-begin-early-implementation>); "New Regulations Implement Significant Expansion of CFIUS Jurisdiction – Mandatory Filings and Civil Penalties," *Wiley Rein LLP*, October 10, 2018. (<https://www.wileyrein.com/newsroom-articles-Alert-New-Regulations-Significantly-Expand-CFIUS-Jurisdiction-by-Requiring-Mandatory-Declarations-for-Critical-Technology-Deals.html>)

codes.<sup>7</sup> According to Treasury, these are “industries for which certain strategically motivated foreign investment could pose a threat to U.S. technological superiority and national security.”<sup>8</sup> The pilot regulations went into effect on November 10, 2018.

Then, on January 13, 2020, Treasury published final CFIUS regulations that address covered investments (both control and non-controlling), real estate transactions, and related mandatory declarations.<sup>9</sup> The regulations will be effective February 13, 2020, and are expected to impact bankruptcy filings as well as other transactions. Of particular interest is the fact that the new regulations are shifting the mandatory declaration process from a focus on NAICS codes and critical technologies to primarily understanding critical technologies through the lens of export control standards. This may affect how the bankruptcy court identifies which proceedings may implicate CFIUS review.

NAICS codes are often provided in bankruptcy filings, although not with any consistency, and unless cross-border exchanges are brought to their attention, the U.S. government lacks visibility into technology and related transfers that occur in the bankruptcy courts.

Although voluntarily chosen by industry members, NAICS codes reflect an entity’s view of its primary business. Companies sometimes use more than one NAICS code, depending upon the circumstances. Export classifications similarly provide useful categorization of the technology at issue. These two pieces of information provide a window into the type of business and the products, services and technology the business handles.

Modification to the Bankruptcy Court process to require such codes in all filings would provide bankruptcy court judges the opportunity to identify technologies that may have national security implications and require proof of export license or CFIUS review.

This focused enhancement to the court’s processes can provide judges with essential information that can help identify technology that raises national security concerns while limiting inappropriate exploitation of technology through the bankruptcy process.

## **2. Provide guidance to judges to utilize existing in camera review, where appropriate, for proceedings that have export-controlled or otherwise sensitive technology at issue.**

Although bankruptcy court judges have limited visibility into the interactions and negotiations leading up to a plan or bid,<sup>10</sup> judges manage their courtrooms during the course of a proceeding. Through that management process, judges can become aware of sensitive information involving

---

<sup>7</sup> “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.” “North American Industry Classification System.” *United States Census Bureau*, accessed October 19, 2018. (<https://www.census.gov/eos/www/naics/>)

<sup>8</sup> U.S. Department of the Treasury, “Fact Sheet: Interim Regulations for FIRRMA Pilot Program,” October 10, 2018. (<https://home.treasury.gov/system/files/206/Fact-Sheet-FIRRMA-Pilot-Program.pdf>)

<sup>9</sup> U.S. Department of the Treasury, “Final rule; and interim rule with request for comments,” January 13, 2020. (<https://s3.amazonaws.com/public-inspection.federalregister.gov/2020-00188.pdf>)

<sup>10</sup> Judges are not permitted to attend meetings with creditors and equity security holders. 11 U.S.C. § 341(c).

the assets at issue, the scope of technology or products involved, and the parties with an interest in purchasing the assets.

Without proactive steps by judges, exposure of controlled or sensitive technology can occur through the discussion of technical information or technology in an open court setting where foreign persons attend. It can also occur in court filings, where specific technology or technical information is discussed in detail as part of the bankruptcy proceedings. When goods, services, and technology are subject to U.S. export controls,<sup>11</sup> access by or release to foreign nationals of these controlled technologies, even in the United States, is considered an “export.”<sup>12</sup> These exports generally require some form of approval prior to release to a foreign person. Without a process for managing the sharing of technical information in an open courtroom or in docket filings, violations of the export regulations,<sup>13</sup> in addition to the improvident release of such information to foreign persons, can occur.

Given the judge’s central role in the proceedings, the court’s rules regarding the engagement involving sensitive information can be logically and more consistently extended to cover technologies that are export controlled or transactions that would be subject to CFIUS review. Ensuring that the court’s rules or procedures expressly address export-controlled technologies as part of the in camera review<sup>14</sup> process, in addition to the protective order process discussed in our third recommendation below, would assist the U.S. government – in a “whole of government” approach – to identify technology transfers that should be limited or that merit further review by agencies with cognizance over the transfers, outside of the bankruptcy proceedings. 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 may be national security concerns regarding the release of any information in open court or through court filings.

### **3. Leverage protective orders to limit access to sensitive technology and intellectual property during bankruptcy proceedings.**

---

<sup>11</sup> Export control authorities do not proactively “seek out companies developing new technologies” or “investigate the relationship between investors and employees of a startup.” M. Brown and P. Singh, “DIUx Study on China’s Technology Transfer Strategy,” Defense Innovation on Unit Experimental (DIUx), page 23, January 2018. ([https://admin.govexec.com/media/diux\\_chinatechnologytransferstudy\\_jan\\_2018\\_\(1\).pdf](https://admin.govexec.com/media/diux_chinatechnologytransferstudy_jan_2018_(1).pdf)). Thus, an extensive amount of technology transfer can occur without accountability. The court system, however, can supplement the management and administration of inappropriate transfers with the collection and sharing of information with U.S. Government stakeholders as part of the bankruptcy process.

<sup>12</sup> “Export” or “release of technology” is defined in the EAR and the ITAR, at 15 CFR § 734.15 and 22 CFR 120.17 and 120.50. These terms have been interpreted in various enforcement actions executed by the Department of Commerce/Bureau of Industry and Security and the Department of State/Directorate of Defense Trade Controls. *See, e.g., Settlement Agreement with Intevac* (BIS, 2017 [CONFIRM]) (provision of passwords to a foreign national employee constitutes a release of technical data and technology if export controlled information resides on the IT systems); *In the Matter of FLIR Systems, Inc.* (DDTC, 2018) (verbal, visual and electronic access to export controlled information by foreign persons, whether in the US or abroad, constitutes and ‘export’); *see also In the Matter of Meggitt USA, Inc* (DDTC, 2013).; *In the of General Dynamics Corporation/General Motors Corporation* (DDTC, 2004).

<sup>13</sup> *Id.*

<sup>14</sup> “In camera (legal).” *West’s Encyclopedia of American Law, edition 2*. 2008. The Gale Group 18 Aug. 2018 ([https://legal-dictionary.thefreedictionary.com/In+camera+\(legal\)](https://legal-dictionary.thefreedictionary.com/In+camera+(legal)))

Federal and state courts have long utilized protective orders to limit public access to sensitive, proprietary, classified, export-controlled, and law enforcement-related information. *See, e.g., Ross-Hime Designs v. United States*, Case No. 11-201 C (COFC) (March 13, 2013) (Protective Order); *United States v. Sixing Liu*, Crim. No. 11-208(SRC (D.N.J. September 4, 2012)(Protective Order); *L'Garde Inc. v. Raytheon Space and Airborne Systems*, \_\_\_F.Supp.3d. \_\_\_ (C.D. Calif. September 14, 2011)(Protective Order); *United States v. Melvin*, 14 Ct. Cl. 236 (1988). These cases recognize that export-controlled information is sufficiently sensitive that it should be expressly addressed in protective orders.

In *Melvin*, an intellectual property dispute where the inventor sought access to controlled Air Force-sensitive information as part of his allegations of IP violations, the court held:

“Because public disclosure of technical data... is ‘tantamount to providing uncontrolled foreign access, the Secretary of Defense may withhold from public disclosure any technical data with military or space application...” 14 Cl. Ct. at 238-239.

The court expressly crafted a protective order designed to address the need to prevent the unrestricted dissemination of export-controlled information in open court.

The Bankruptcy Courts have individually, though inconsistently, recognized the importance of protective orders when handling export-controlled information. For example, the Bankruptcy Court in the Southern District of New York implemented a protective order in the Iridium proceedings that directed the limited distribution and handling of export-controlled information.<sup>15</sup> There is, therefore, some precedent for recognition by the Bankruptcy Courts that protective orders are essential when dealing with export-controlled information and can be applied to sensitive technologies that have dual uses.

## CONCLUSION

Leveraging these tailor enhancements to existing tools, as outlined, can help limit the circumvention of national security protections such as a CFIUS review or the export licensing process. The judiciary has an important role to play in the identification and protection of relevant technologies prior to their transfer to a foreign party. Implementing the recommendations will go a long way to support a whole of government effort to advance national security.

DB1/ 110934766.1

---

<sup>15</sup> *In the Matter of Iridium Operating LLC v. Motorola, Inc. and Official Committee of Unsecured Creditors of Iridium*, 329 B.R. 403 (Bkr. SDNY 2005). The (Iridium bankruptcy proceeding included “thousands of boxes of documents that had been produced, over 70 depositions, and over 2,000 exhibits marked in connection with the depositions, under the existing terms of the protective order and that ... included information governed by United States export control laws.” *Id.* at 406).