AMERICAN BANKRUPTCY INSTITUTE

2020 Virtual Winter Leadership Conference

Navigating Distressed Investing, Sales and Technology: Protecting Your Sale Process, Your Investments and Your Hide

Presented by the Emerging Industries and Technology & Secured Credit Committees

Dylan Trache, Moderator
Nelson Mullins Riley & Scarborough LLP | Washington, D.C.

Solymar Castillo-Morales
Goldman Antonetti & Cordóva, LLC | San Juan, P.R.

Louis T. DeLucia
Ice Miller LLP | New York

Prof. Harvey Rishikof
Temple University Beasley School of Law | Philadelphia

CONCURRENT SESSION

2020

DISTRESSED INVESTMENT GROUP

A Secured Lender's Perspective
Distressed Sales of Intellectual Property

IceMiller LEGAL COUNSEL | icemiller.com

Louis T. DeLucia
Ice Miller LLP

Secured Parties

- Asset based lenders
- DIP lenders
- Mortgagees
- Syndicated lenders
- Mezz debt lenders
- Other secured parties, and
- Purchasers of the secured party's interests

IceMiller LEGAL COUNSEL | icemiller.com

Acquisition and Investment in Distressed Assets

- § 363 sales
  - "Highest and best bid," which does not always mean the highest price
  - CFIUS compliance, as applicable
- Secured lender "credit bids" or "loan to own" (including DIP loans)
- Conversion of debt to equity transferring ownership under a plan (debt greater than value of assets – fulcrum debt).
- Acquisition of distressed debt to acquire ownership
- Other distressed asset or debt sales
  - Foreclosure
  - Receiverships
  - ABCs
- Concern: CFIUS compliance trigger

IceMiller LEGAL COUNSEL | icemiller.com

Key Terms

- "CFIUS" – Committee on Foreign Investment in the U.S. (1975)
- "FIRRMA" – Foreign Investment Risk Review Modernization Act, August 13, 2018, along with its regulations passed by US Treasury Department, which became effective February 13, 2020
- "Foreign Government Controlled" investor, purchaser, or lender
- "FDI" – Foreign direct investment
- "Covered Transaction" or "Covered Investments" - Non-controlling investments in US businesses engaged in specified TID US Businesses
- "Covered Real Estate Transactions" – the purchase or lease by, or concession to a foreign person of real estate within proximity of US airports, maritime ports and military facilities
- "TID" or "TID US Businesses" -- critical technologies, critical infrastructure, or sensitive personal data ("technology, infrastructure and data" in US companies)
- "Excepted Real Estate Foreign States" – UK, Canada, and Australia
- "Safe Harbor" – When CFIUS or the President have completed all required actions relating to a covered transaction and announced a decision to not exercise authority with respect to the transaction, the parties receive a "safe harbor" with respect to that transaction. 31 C.F.R. § 800.508(d)

IceMiller LEGAL COUNSEL | icemiller.com

Covered Transactions

Extension of a loan or a similar financing arrangement by a foreign person to a US business, regardless of whether accompanied by the creation in favor of the foreign person of a secured interest over securities or other assets of the US business, shall not, by itself, constitute a ***covered transaction****. §800.306*

CFIUS review will trigger because of imminent or actual default or other condition, there is significant possibility that the foreign person may obtain ***control of a US business, or acquire equity interest and access, rights, or involvement …over a TID US Business, as a result of the default or other condition****.*

A covered transaction may include a loan accompanied by financial governance rights characteristic of an equity investment but not typical of a loan. A ***covered real estate transaction*** *may include a real estate loan secured by property in a certain location, e.g. certain U.S. ports, airports, sensitive government locations, and the default provisions (where lender may take title) could trigger CFIUS compliance issues.*

IceMiller LEGAL COUNSEL | icemiller.com

Remedies Upon Default

Practice TIP: Draft in advance to avoid road blocks and delays down the road. Use structures (a) that do not transfer equity (like convertible debt instruments) or control to foreign investor/lender, who may be passive beneficiary of entity exercising control, and (b) include borrower representations as to its status as a TID US Business, etc.

- May trigger CFIUS compliance issues if foreign lender obtains sole or controlling interest over the US borrower/business (if foreign lender is part of a syndicate, but thus not controlling remedies as to the US borrower, because it needs the consent of US participants to act, it may not trigger CFIUS compliance requirements)
- UCC and Mortgage Foreclosure (including strict foreclosure)
- UCC Article 9 self-help remedies and private sales
- Bankruptcy Code remedies (credit bid, stay relief, debt to equity conversion, adequate protection, other remedies)
- Consider a restructuring transaction that gives the foreign lender subordinated debt (or similar leverage) in lieu of equity which would trigger CFIUS review.
- Consider appointment of US person such as a CRO (chief restructuring officer) or independent fiduciary (e.g. receiver or trustee) or transfer control to another US control person upon or prior to default
- Consider contacting CFIUS Committee and request advice regarding jurisdiction and concerns

If US business of the foreign person is controlled by a US person, the Committee (CFIUS) will take that into consideration when determining if the transaction is a "**covered transaction**".

IceMiller LEGAL COUNSEL | icemiller.com

Repercussions of Failure to Comply with CFIUS

- Forced divestiture
- Imposition of mitigation requirements
- Penalties

IceMiller LEGAL COUNSEL | icemiller.com

Louis T. DeLucia

1500 Broadway 29th Floor New York, NY 10036
louis.delucia@icemiller.com
p: 212-835-6312
f: 212-835-6322

Louis T. DeLucia is a partner in and chair of Ice Miller's national Bankruptcy & Restructuring Practice, focused on providing clients facing distressed situations with creative, strategic and cost-effective solutions that both minimize risk and maximize areas of potential opportunity and recovery.

Chambers USA reported that "Louis DeLucia offers clients experience in all areas of insolvency, corporate debt restructuring and bankruptcy litigation. His ability to isolate key issues in a case is highlighted by clients as a major asset of his practice."

Louis has successfully represented a diverse group of clients that includes leading financial institutions; agents for bank syndicates; DIP lenders; indenture trustees; unsecured creditors' committees; equity committees; asset purchasers; lenders to franchisors and franchisees; hedge funds; private equity funds; bondholders; governmental entities; corporations and shareholders; trustees, receivers and assignees; and debtors and creditors.

Louis is also a founding member of Ice Miller's Distressed Investment Group ("DIG"), which focuses on distressed investment strategies and transactions, including bankruptcy and in-court restructurings, out-of-court restructurings, and other insolvency-related transactions. Louis has more than 30 years of experience in advising clients on complex strategic investing in the distressed market, including advising on loan-to-own strategies, debt restructurings, debtor-in-possession and exit financings, claims trading, distressed real estate acquisitions, section 363 sales, rescue capital deployment and other investment situations. For more information on DIG, please see https://www.icemiller.com/distressed-investments/.

IceMiller LEGAL COUNSEL | icemiller.com

Data privacy and security issues, protection of sale information, virtual data rooms, and COVID orders affecting these processes.

Data privacy is how you collect, share, and use data, while data security refers to how you protect your data from internal and external attackers. Data privacy is not possible without data protection.

The United States and most countries worldwide have enacted legislation concerning data privacy in a sectorial manner, which means that it has created each law or regulation in response or compliance to the needs of a particular industry or section of the population. We can mention the Electronic Communications Privacy Act (ECPA), which extends government restrictions on wiretaps to include transmissions of electronic data; the Video Privacy Protection Act, that prevents wrongful disclosure of an individual's personally identifiable information stemming from their rental or purchase of audiovisual material, and the Gramm-Leach-Bliley Act, which mandates how financial institutions must deal with the private information of individuals. Also, the Sarbanes_ Oxley Act (SOX) 2002 protects the public from fraudulent practices by corporations, the ISO 27001 (2012) functions as a framework for information security. The GDPR (2018) General Data Privacy Regulation, aims to protect the European Union citizens' personal data and imposes on the companies to undertake several tasks such as requesting explicit opt-in consent from users, the users' right to request data from companies, and the right to have your data deleted. Some states in the US, like California and New York, have also enacted specific legislation to protect the disclosure of information of their citizens. Also, the federal Defend Trade Secrets Act (DTSA) protects "trade secrets" defined as "all forms and types of financial, business, technical, economic, or engineering information" that (1) derive independent economic value from not being generally known to, and not being readily ascertainable through proper means by, another person who can obtain economic value from it; and (2) the owner has taken "reasonable measures" to keep secret. In other words, under federal law, a "trade secret" has two components: economic value and secrecy. Most states have their own trade secret statutes with identical or similar definitions of "trade secret."

The worldwide lockdown put the enforcement of all those statutes to the test. Everyone needed to increase security measures to safeguard the information while working from home. The lockdown orders issued worldwide, some of which remain in effect today, significantly increased the professionals working away from the office, bringing sensitive information and files outside of the corporate firewall. In this process, they are using many web-based or on-demand applications and cloud services. These developments demand more security on the remote work platforms. But this security enhancement is necessary for the digital storage of the information; the security on the physical handling of the data also needs improvement.

At the beginning of the Pandemic, most companies were stuck with limited remote access tools. Usually, this included a Virtual Private Network (VPN) and basic anti-malware/antivirus software, which provided a certain level of protection to restricted or partial remote access to their office applications and systems. A VPN is a private, encrypted

channel that will allow employees to directly access a company's network while significantly minimizing the risk to the company's confidential information and trade secrets. VPNs are also beneficial as they allow employers to create and monitor remote workers' access logs that track files as they are opened, used, and transmitted by each employee. As the spectrum of remote work expanded, vulnerabilities and risks to hackers' attacks on private or confidential information increased.

Several consultants[1] pointed as an example that at-home employees of financial institutions have the regulatory need to ensure that transactional communications with each other and with customers are handled on a private, highly secure infrastructure. The remote work increased the risks of security breaches. The companies need always-on surveillance and real-time risk analysis for breaches at both physical and digital entry points. Company leaders, managers, and their staffs need access to internal services and applications so they can conduct operations remotely. Since many companies have not made these applications and data available previously over the Internet or virtual private networks (VPN), security leaders are reluctant to allow access without stringent access mechanisms.

Understandably, when the governments of different countries-imposed lockdowns, very few organizations were prepared for their workforces to be working remotely in mass. Secure remote-access capacity and secure access to enterprise systems have become a significant constraint. Also, these accesses are expensive and not believed where remote work was not the norm. Therefore, even where numerous entities had remote access available, it was not meant for the entire workforce of a company, at least, not at the same time. Increases in the use volume rest the operations unmanageable as it slows down the access to information.

Some businesses have had to allow employees to use their personal digital devices to access enterprise applications without any mechanism for enforcing security controls to continue providing services. Even when the employees have access to the applications through VPNs, not necessarily perform their work in and through the business platforms; therefore, they are at risk of data security infringement. For most organizations, business continuation plans (BCP) and incident response plans (IRP) are inadequate or even nonexistent to deal with the fact that they need work to perform out of the premises during pandemics.

The lockdown required the companies to take reasonable measures to ensure the business's continuity without compromising the safety of their data. For lawyers, when talking about reasonable measures, it means doing your due diligence in choosing your providers. Including the industry norms, determining the provider's security precautions such as firewalls, password protection, and encryptions, the provider's reputation and history, asking for any breaches, and inquiring that the provider follows confidentiality requirements, and requiring that the data is under the lawyer's control of the lawyers. *See* Iowa State Bar Ass'n Op. 11-01, (2011).

[1] Such as TATA Consulting Services, *see* How COVID- 19 is dramatically Changing Cybersecurity. https://www.tcs.com/content/dam/tcs/pdf/perspectives/covid-19/How%20Covid-19%20is%20Dramatically%20Changing%20Cybersecurity.pdf Last Seen 11/10/2020.

In summary, offices need to ensure that the services and programs implemented comply with industry norms and the legal standards for confidentiality and privilege in your jurisdiction and are secured to avoid a breach. *See* ABA Comm. On Ethics & Prof'l Responsibility, Formal Op. 477R (May 22, 2017).

> A Lawyer may send client information over the Internet if lawyer makes reasonable efforts to prevent inadvertent or unauthorized access, but may be required to take special security precautions when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (May 22, 2017)

In the *Formal Op. 477R*, the Committee adopted the language of the ABA Cybersecurity Handbook as to what should be considered the reasonable efforts standard. It concluded that, in an environment of increasing cyber threats, instead of imposing specific security measures, the law firms should:

> "adopt a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments."

Citing Jill D. Rhodes & Vincent I. Polley, The Aba Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals 7 (2013) note 3, at 48-19.

As cyber-threats have increased and electronic communications devices have proliferated, it is not always reasonable to rely on the use of unencrypted email. Electronic communication through specific mobile applications or on message boards or via unsecured networks may lack the basic expectation of privacy afforded to email communications. Therefore, lawyers must, on a case-by-case basis, continuously analyze how they communicate electronically about client matters, applying the Comment [18] factors to Model Rule 1.6 to determine what effort is reasonable. *See* ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (May 22, 2017)

It is critical to be aware that cybercriminals use heightened digital footprint and traffic to find vulnerabilities. As the remote through-internet work increases, they are launching Covid-19-themed attacks in the form of phishing emails with malicious attachments that drop malware to disrupt systems or steal data and credentials. Attackers are creating temporary websites or taking over vulnerable ones to host malicious codes. They lure people to these sites and then drop malicious code on their digital devices. Remote working tools such as videoconferencing systems have also been hacked for vulnerabilities.

According to TATA Consulting Services' recommendations, an integral approach to the success of security efforts would be deploying technologies and solutions that are effective and quick to adopt, such as those that are hosted in the cloud. Cloud-based security and

platform services markedly reduce deployment time. They also let companies increase the breadth and depth of security protection rapidly (i.e., referred to as dynamic scalability), depending on the moment's threats. Experts refer that cloud-based security also enables IT, security professionals to manage all this remotely. The cloud is also key to security systems. Secure-edge, cloud-based data leakage prevention, and threat-protection controls can help safeguard an organization's critical assets. Moreover, cloud-based managed detection and response services can be extended to remote workplaces.

Additionally, companies that use secure remote access technology can give remote employees private access, without a Virtual Private Network (VPN), to enterprise applications and systems. Firms can also use privileged access management (PAM) services to allow special remote access to their IT and application administrators. Multi-factor authentication services, including biometric and text-based methods, enable stringent risk-based access to internal applications that are opened for remote access.

Information Technology consultants agree that as the remote work environment is part of the new normal, the companies will be forced to optimize their digital transformations featuring "near -zero latency on multiple dimensions: data, provisioning, activation, tracking, network, security, compliance, program, management, transition and service-level agreements." Experts have provided Business-Focused Data Privacy Tips[2] for the companies to follow, such as:

- Cybersecurity and IT rights will require careful examination and handling. Remote workers' monitoring and support will become vital.
- Reassess systems and data access rights, IT systems will need to be analyzed for cracks, foul paths, or fraudulent identities regularly.
- Analysis of new cyber risks and scrutinize the digital capabilities of the critical business functions to make sure that it can withstand an attack during lockdowns.
- Reassessing the corporate IT security architecture; access mechanisms, support for remote access on volume or mass scale (at least for the whole entity), and security authentication mechanisms.
- Update remote access continuously and clean up personal devices. (Hygiene controls)
- Monitor your network for suspicious activity so that you can catch on to an attack early enough to reduce the damage. Train employees to recognize and report malware, phishing emails, and other internet scams that target computers and other electronic devices where the company information is stored.
- Ensure that every employee at the company is aware of data security and privacy concerns and techniques. Integrate training on data privacy into the general training program. Update, discuss, and make sure that your employees understand the remote or telework policy. Specify the steps the employees should take to guarantee the

[2] Data Privacy Guide- Definitions, Explanations and Legislations- Varonis, https://www.varonis.com/blog/data-privacy/ last seen 11/10/2020.

protection of confidential information. Urge and always remind the importance of maintaining confidentiality obligations.

- Make sure that you take advantage of the free security tools that are out there, including encrypted storage solutions, password managers, and VPNs. These small tools can dramatically decrease your company's vulnerability to attack and are easy to use and install.
- Do not underestimate hackers' interest in your company because it is smaller or just starting— breaches and attacks affect organizations of all sizes, including start-ups and small businesses.
- Implement the zero-trust model. As Sivan Tehila, founder of Leading Cyber Ladies and Cyber19w, tells us, "Zero Trust restricts access to the entire network by isolating applications and segmenting network access based on user permissions, authentication, and user verification. With Zero Trust, policy enforcement and protection are easily implemented for all users, devices, applications, and data, regardless of where users are connecting from. This user-centric approach makes the verification of authorized entities mandatory, not optional. This 'trust but verify' mindset is essential for today's organizations."
- Adopt advanced technology and insurance policies against losses from cyberattacks.

See also TATA Consulting Services. https://www.tcs.com/cyber-security-services. Last seen 11/10/2020.

Other leaders in the field, such as Citrix, understand that using the zero-trust model to endpoint security has become one of the most successful strategies for securing flexible or hybrid workforces (including remote work) for the long term. As explained in one of its multiple articles,[3] the process starts with the assumption that every endpoint must be secured not only at sign-on but continuously as well--as the employee uses apps and services. This represents a significant change from the old approach of VPN accesses. The shortcoming of the VPN has become manifest now with extensive use of remote work; anyone, whether a user or an adversary, who has access to a VPN tunnel from a remote computer to your network, has access to everything. One key can unlocks an entire network.

The zero-trust model itself is enhanced by using artificial intelligence (AI) and machine learning (ML). Intelligence enables the secure platform to analyze all aspects of every worker's interactions in real-time and searches for anomalies, making it possible to stop attacks as they are occurring rather than after the fact. Intelligent tools combine data from key points such as IP address, files accessed, activities, apps being used, and more to immediately identify any out-of-bound activities or suspicious interactions that stray from the baseline behaviors of the individual, known in every detail by the intelligent tool. This modern approach to securing remote work improves dramatically defensive posture. And perhaps more importantly, it

[3] Remote Work Demands a Zero-Trust Approach for Both Apps and Users, https://searchenterprisedesktop.techtarget.com/futureofwork/Remote-Work-Demands-a-Zero-Trust-Approach-for-Both-Apps-and-Users?_ga=2.264382409.794969829.1604976562-1789979084.1604976562. Last reviewed on 11/09/2020.

protects both workers and applications, which is a significant cybersecurity trend. Moving away from a device-centric perspective and focusing on behaviors of apps and workers delivers a much more substantial level of cybersecurity.

In addition to the recommendations above, it is also stressed that the companies develop comprehensive customized protocols for remote access, ensuring that only authorized users- on a need to know basis only – access the systems, databases, and networks. Employers should require employees to, at least, use secured connections, such as VPNs and two-step authentications, or similar protective measures.[4] In addition to the digital access restrictions, the companies must ensure security for the handling of hard-copy documents. The companies must establish specific protocols, such as prohibiting printing or reproducing certain materials, requiring locked cabinets to secure information, not in use, and the return or proper destruction of the data.

Virtual Data Rooms and Virtual Meeting Rooms.

Virtual Data Rooms (VDR) is a type of online database used for storing and sharing documents with only authorized users' access. Key players to this enterprise, to name a few, are Ideals Solutions Group, Citrix Systems, SecureDocs, Safelink Data Rooms, Sharevault, Caplinked, EhtosData, IdrShare, Sterling, Intralinks, HighQ Solutions, and SmartRoom. This sharing room does not substitute the companies' obligations to safeguard the confidentiality of the information stored in those rooms. It is essential to emphasize the execution of non-disclosure agreements (NDA) and the consistent designation of confidential information to secure not sharing the material available through these virtual data rooms with non-authorized parties or entities. The parties must stress that NDAs are not only executed but followed.

The organizations also need to apply and enhance the same cybersecurity and data protection policies to the virtual meeting platforms. It is crucial to review user instructions, terms and conditions, and privacy policies for each platform and implement the protective measures for those meeting services.

Some potential risks on the virtual meeting services are: 1) the risk of uninvited third parties joining the meeting and see confidential information. To safeguard this risk, the hosts may require users to access sessions with a password and generating meeting IDs only disclosed to the invitees, and closing the meeting after all invitees have joined; 2) Unwanted disclosure of confidential content. To avoid that, the host may limit access to share screens. 3) Also, the host may notify and obtain the participants' consent, to record the video or audio of the meeting. If a recording is prohibited, the host shall also state it in writing before the meeting

[4] Igor Babichenko, Rodney Satterwhite, McGuireWoods LLp, Protecting Business Information During COVID-19 Pandemic. April 16, 2020. https://www.jdsupra.com/legalnews/protecting-business-information-dur. Last Seen on 11/11/2020.

starts. 4) it also suggested that only use platforms with terms and conditions that limit the use of user's content. [5]

Court Orders during COVID-19 Pandemic

To varying degrees before the Pandemic, courts had been using online processes like electronic filing, online case management, video- and teleconference hearings, online payment platforms, text message notifications, and Online Dispute Resolution (ODR). These technologies acted as gateways to modernization that this Pandemic has accelerated. As a direct result of the Pandemic, courts have improved their business processes and increased access for court users by deploying remote services to conduct essential functions and provide greater flexibility for court users and staff alike. While some of these solutions have been tested and proven for years, the disruptive Pandemic expedited the courts' use of them and diminished the change's resistance.[6] These technological improvements provide benefits beyond this Pandemic, as these same solutions allow state courts to prepare disaster plans to maintain court operations during other challenges, such as power outages, natural disasters, or cybersecurity attacks. As court processes become increasingly intertwined with technology, disaster plans must create redundancies to address situations that may specifically impact mission-critical technologies. The Post-Pandemic Planning Technology Working Group of the Conference of Chief Justices/Conference of State Court Administrators has made recommendations to embrace technology and make it accessible to the public in the long run.

Federal courts are individually coordinating with state and local health officials to obtain local information about the coronavirus (COVID-19) and have issued orders relating to court business, operating status, and public and employee safety. COVID-19 has been more focused on extensions of deadlines and delimiting which platforms are being used than restricting the use of virtual rooms, which has enabled the continuance of business deals and discovery processes.

The National Center for State Courts has informed that the five most common efforts taken by the courts to combat the coronavirus are:

- Retracting or ending jury trial
- Generally suspending in-person proceedings
- Restricting entrance to courthouses
- Granting extensions for court deadlines, including the deadlines to pay fees/fines, and
- Encouraging or requiring teleconferences instead of hearings

In Puerto Rico, for example, the last order, issued on November 6, 2020, indicated that the District Court would continue to use its video teleconferencing ("VTC") or teleconference systems (mainly Zoom and Court Solutions) to hold eligible civil and criminal proceedings

[5] Kevin Pomfret, Williams Mullen. Protecting Your Sensitive Information While Using Virtual Meeting Platforms. April 7, 2020. https://www.jdsupra.com/legalnews/. Last seen 11/10/2020.
[6] Guiding Principles for Court Technology, July 16, 2020, Version 1. National Center for State Courts. https://www.ncsc.org/newsroom/public-health-emergency. Last seen 11/10/2020.

until January 11, 2021. Nonetheless, with the Chief Judge's approval, certain critical in-person proceedings may be held by way of exception. The same instructions apply for the Bankruptcy Courts but do not necessarily use the same virtual platforms. The Bankruptcy Court for the District of Puerto Rico notified in its Notice 20-21 that, beginning on November 16, 2020, the court will conduct all hearings via Microsoft Teams instead of Skype for Business.

Commentaries and General Recommendations:

To protect your information from Cyberattacks is an ongoing concern. Cyberattacks evolve at high speed, and besides the company's enhancement of its security systems, the best way to maintain such a level of security is to bring it to the employees' awareness and responsibility.

As professionals working from home have become an essential component of business transactions, the exposure and risks for the confidential and private information of business deals be accessed by unwanted third parties is impending. Therefore, the companies must ensure that enhanced security measures are taken within the networks accessed by their remote- working professionals, but also that their employees also take steps to protect their home accesses. Companies must continuously remind and guide their employees to identify phishing activities and scams that, once entered into the personal computer, may have access to the companies network and must establish procedures for the employees to report it.

An effective way to guide this remote work environment might be as easy as sending biweekly or monthly emails reminding and updating the Red Flags and Dos and Don'ts of accessing web-based information, emails, or accepting internet correspondence.

Several consultants agree, and we must remind our professionals of this most common RED FLAGS found on phishing emails:

* Does the email ask for any sensitive/personal information (password, credit cards, SSN, etc.)?

* Does the email request for sensitive information about others?

* Does the email ask you to act or open an attachment to avoid account closure immediately?

* Does the hover-text link match what is in the text?

* Does the address in the 'To' field match the sender of the email?

The senders of most of those emails appear as your referenced counterparties in your personal and working environment and even can seem as follow up emails. They also recommend avoiding and to DO NOT replying to, open attachments from, or click on URLs from unknown and untrusted sources. Avoid the use of your company email address for personal communications. Never send personal/sensitive information via email—e.g., passwords, credit card number, social security number, or account number.

You must also watch for misspellings, grammatical errors, and abnormal spacing that may indicate a phishing email. Check links by using your mouse to hover over the hyperlink to determine if the URL makes sense with the sender—e.g., matching the sender name to the URL; whether there's a foreign name or location in the URL.

Always use common sense; if it does not look right, trust your judgment; and report any suspicious emails—even if you are not sure—to your manager and IT Security.

As a recent example, I received an email with alleged invoices for the virtual data room and a discovery process in the TITLE III Proceedings for the Commonwealth of Puerto Rico. The email seemed sent by one of the multiple attorneys appearing in the case. Several of the computers from attorneys, in that case, got infected with a virus. The sender's email address was a slight, almost imperceptibly different from the counsel's email appearing in the case. Another counsel warned me before I opened the email, but I did not notice. In my case, the email went to the junk file, but one of the policies in our law firm is to review the junk file for emails erroneously directed to that folder by our firewalls.

Therefore, managing cybersecurity issues is a matter of being aware of what you receive and access. Once you grant access to an unwanted visitor, you can be jeopardizing not only your company's security but the information entrusted to you by your clients.

Solymar Castillo-Morales
Goldman, Antonetti & Córdova, LLC.
ABI Winter Leadership Summit
Panel: Navigating Distressed Investing, Sales and Technology: Protecting Your Sale Process, Your Investments – and Your Hide.
November 13, 2020

Bibliography

1. A readable Thread by @chris_herd Says I've spoken to around 1,000 co... https://unrollthread.com/t/1313202750818312192/. Last seen 11/10/2020
2. Data Privacy Guide: Definitions, Explanations, and Legislation | Varonis https://www.varonis.com/blog/data-privacy/ Last Seen 11/10/2020.
3. E-Commerce in the times of COVID-19, Tackling Coronavirus (COVID-19): Contributing to a global effort. Oecd.org/coronavirus October 7, 2020.
4. Formal Opinion 2019-2: Use of a Virtual Law Office by New York Attorneys. https://www.nycbar.org/member-and-career-services/committees/reports-l..., May 15, 2019. Last seen on 11/10/2020.
5. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 477R (May 22, 2017)
6. Guiding Principles for Post-Pandemic Court Technology. A pandemic resource from CCJ/COSCA. July 16, 2020, | Version 1 National Center for State Courts. https://www.ncsc.org/newsroom/public-health-emergency. Last seen 11/10/2020.
7. How COVID- 19 is dramatically Changing Cybersecurity, Prashant Deo, Geetali Raj and Ramesh Perumal, TATA Consulting Services, www.tcs.com.

8. Leading Sales Through the COVID-19 Crisis | BCG https://www.bcg.com/publications/2020/stabilize-increase-sales-through. Last seen 11/10/2020.
9. Order DE28 District of Puerto Rico
10. Engstrom, David Freeman, Post-COVID Courts (September 1, 2020). 68 UCLA L. Rev. Disc. 246 (2020), Available at SSRN: https://ssrn.com/abstract=3684865 or http://dx.doi.org/10.2139/ssrn.3684865
11. US Data Protection Compliance & Regulations Whitepaper, Varonis https://www.varonis.com/blog/data-privacy/ Last Seen 11/10/2020.
12. Impact of COVID-19 Outbreak on Virtual Data Room (Software) Market https://wiseguyreports.wordpress.com/2020/08/07/impact-of-covid-19-outbreak-on-virtual-data-room-software-market-2020/. Last seen on 11/11/2020
13. McGuireWoods LLP, Protecting Business Information During the COVID-19 Pandemic, April 16, 2020
14. Impact of COVID-19 Outbreak on Virtual Data Room Software Market ... https://wiseguyreports.wordpress.com/2020/09/28/impact-of-covid-19-outbreak-on-virtual-data-room-software-market-2020/. Last seen on 11/11/2020
15. Kazim Naqvi, Sheppard Mullin Ritcher & Hampton, LLP. 4 Steps to More Effectively Use NDAs to Protect Confidential Information. April 9, 2020. https://www.jdsupra.com/legalnews/4-steps-to-more-effectively-use-ndas... Last Seen 11/10/2020
16. Ruth Prominslow, Katherine Rusk, Bennet Jones LLP, COVID-19, and Cybersecurity Scam Alert: Protecting Your Information and assets. March 20, 2020, https://www.jdsupra.com/legalnews/covid-19-and-cybersecurity-scam-alert/ Last seen 11/10/2020.
17. Kevin Pomfret, Williams Mullen. Protecting Your Sensitive Information While Using Virtual Meeting Platforms. April 7, 2020. https://www.jdsupra.com/legalnews/. Last seen 11/10/2020.
18. Rachel Churchill, Leigh Gilligan, and Cynthia Keliher. Negotiating Purchase and Sale Agreements During The COVID-19 Pandemic. March 30, 2020, https://www.jdsupra.com/legalnews/negotiating-purchase-and-sale-47644/ Last seen 11/09/2020.
19. Brodie Erwin and Michael Matula, COVID-19 & Cyber Security: Protecting Trade Secrets and Confidential Information During the Telework Boom. May 21, 2020. https://www.jdsupra.com/legalnews/covid-19-cyber-security-protecting. Last seen 11/09/2020
20. Shannon T. Murphy, Winston & Strawn, LLP. 10 Questions Companies should address for a remote work environment. https://www.winston.com/en/thought-leadership/10-questions-companies-should-address-for-a-remote-work-environment.html. Last seen 11/05/2020

Deliver Uncompromised

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

Chris Nissen, John Gronager, Ph.D.,
Robert Metzger, J.D., Harvey Rishikof, J.D.

MITRE

This document is intended to serve as a MITRE Advisory Document for the United States Government to aid in the formation of a holistic strategy for dealing with supply chain security within the Department of Defense. It is not intended to be an Implementation Plan with specific Lines of Effort (LOE). Rather, the recommended Courses of Action presented here, in addition to others, would comprise the LOEs in such a plan. It is intended to address how supply chain security as a part of acquisition of capability can be holistically approached.

Approved for Public Release. 18-2417. Distribution unlimited. August 2018

Deliver Uncompromised

A Strategy for Supply Chain Security and Resilience in Response to the Changing Character of War

Chris Nissen
John Gronager, Ph.D.
Robert Metzger, J.D.
Harvey Rishikof, J.D.

August 2018

The MITRE Corporation.

MITRE

Executive Summary

The character of war is changing. Our adversaries no longer have to engage the United States kinetically. They have shifted their strategy to engage our nation *asymmetrically,* exploiting the seams of our democracy, authorities, and even our morals. They can respond to a kinetic action non-kinetically and often in misattributed ways through *blended operations* that take place through the supply chain, cyber domain, and human elements.[1] They can render our national capability to project power—hard or soft—non-mission ready and collapse and even reverse the decision cycle.

Deliver Uncompromised

"For mission owners, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded or inappropriately given away or sold."

William Stephens, Director of Counterintelligence, DSS

Today, various parts of the Department of Defense (DoD) and the Intelligence Community (IC) are generally aware of cyber and supply chain threats, but intra- and inter-government actions and knowledge are not fully coordinated or shared. Few if any holistically consider the entire blended operations space from a counterintelligence perspective and act on it. Risk quantification and mitigation, as a mission, receive insufficient resources and prioritization. Too little attention is directed toward protection of operational security or software assurance. There is no consensus on roles, responsibilities, authorities, and accountability. Responsibilities concerning threat information are "siloed" in ways that frustrate and delay fully informed and decisive action, isolating decision makers and mission owners from timely warning and opportunity to act.

DoD must make better use of its existing resources to identify, protect, detect, respond to, and recover from network and supply chain threats. This will require organizational changes within DoD, increased coordination with the IC, and more cooperation with the Department of Homeland Security and other civilian agencies. It will also require improved relations with contractors, new standards and best practices, changes to acquisition strategy and practice, and initiatives that motivate contractors to see active risk mitigation as a "win." Risk-based security should be viewed as a profit center for the capture of new business rather than a "loss" or an expense

1 The four primary attack vectors in an asymmetric blended operation are supply chain (software, hardware, services), cyber-physical (cyber systems with real-time operating deadlines including weapons systems and industrial control systems), cyber-IT (informational technology), and human domain (witting or unwitting; foreign intelligence service or insider). Most operations use more than one of these vectors to realize an operational effect, moving between them as a function of time as access and opportunity allow. Viewing only cyber-IT as the primary vector affords the adversary a great degree of obfuscation and opportunity in the other three.

harmful to the bottom line. While DoD cannot control all the actions of its numerous information system and supply chain participants, it can lead by example and use its purchasing power and regulatory authority to move companies to work with DoD to enhance security through addressing threat, vulnerabilities, and consequences of its capabilities and adapt to dynamic, constantly changing threats.

Improved cyber and supply chain security requires a combination of actions on the part of the Department and the companies with which it does business. Through the acquisition process, DoD can influence and shape the conduct of its suppliers. It can define requirements to incorporate new security measures, reward superior security measures in the source selection process, include contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments. Of course, there are limitations on what DoD can accomplish. DoD is not so large a customer that it can control all parts of its supplier base. DoD has strongest influence over companies with which it contracts directly. Nonetheless, DoD spending is a principal source of business for thousands of companies. The Department can reward the achievement, demonstration, and sustainment of cyber and supply chain security. It will take time to establish workable, fair processes, but these efforts should be given high priority. Where justified by urgent circumstances, the Department should consider use of interim rules to effectuate *Deliver Uncompromised* (DU) in near-term procurements.[2] By adding more security measures to the acquisition toolkit and making better use of those measures, DoD can exercise security leadership through use of its contractual leverage. This issue is elaborated more fully in *Annex I* of this report.

To succeed with *Deliver Uncompromised* requires commitment at the *enterprise* rather than the *element* level—for the Department and for its contractor base. Given the threat environment and its consequences for DoD, this report identifies a number of strategic elements—courses of action (COAs)—to address the cyber and supply chain security challenge. The COAs collectively can form an Implementation or

2 The genealogy of the term "Deliver Uncompromised" began at a 2010 National Counterintelligence Policy Board meeting when Bill Stephens of the Defense Security Service (DSS), along with National Security Agency CI representative Alan Brinsentine, coined the phrase during an informal conversation. Both were concerned that the U.S. government tolerated contract firms that repeatedly delivered compromised capabilities to DoD and the IC. A few months later, the National Counterintelligence Executive Senior Policy Advisor, Mr. Harvey Rishikof, joined in the conversation. The concept was developed at DSS CI and validated by their counterintelligence collection and analysis program largely built upon the rich reporting of suspicious contacts from cleared industry. Further conversations between the DSS CI leadership and affected government and contractor professionals eventually led to a DSS article in the American Intelligence Journal (Vol 29, no 2, 2011), entitled "The T-Factor and Cleared Industry." DSS CI continued to explore the concept until the organization rolled it out as a panel topic at the DSS 2016 Foreign, Ownership, Control and Influence annual meeting. The Undersecretary of Defense for Intelligence then joined with DSS in a contractor-facilitated DU conversation with likely U.S. government and industry stakeholders. The Office of the Secretary of Defense (OSD) and DSS brought this conversation to this MITRE study effort in order to help DoD find a solution to better maintain its technological advantage.

Campaign Plan that could operate along roughly eight lines of effort: Elevate, Educate, Coordinate, Reform, Monitor, Protect, Incentivize, and Assure.

This report examines options that span legislation and regulation, policy and administration, acquisition and oversight, programs and technology. Actions are presented for the near, medium, and long terms—recognizing the need for immediate action coupled with a long-term commitment and strategy. Cyber and supply chain vulnerability extends well beyond DoD, across government and into the private sector. Nonetheless, DoD has potentially decisive influence in this space. Beyond DoD, actions in the legislative domain are critical, as our adversaries are actively exploiting seams and shortcomings in areas such as information sharing, threat detection, and acquisition transparency. Building effective deterrence to asymmetric threats will require time and deliberate planning. The 15 COAs are:

1. Elevate Security as a Primary Metric in DoD Acquisition and Sustainment
2. Form a Whole-of-Government National Supply Chain Intelligence Center (NSIC)
3. Execute a Campaign for Education, Awareness, & Ownership of Risk
4. Identify and Empower a Chain of Command for Supply Chain with Accountability for Security and Integrity to DEPSECDEF
5. Centralize SCRM-TAC with the Industrial Security/CI mission owner under DSS and Extend DSS Authority
6. Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations
7. Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software
8. Advocate for Litigation Reform and Liability Protection
9. Ensure Supplier Security and Use Contract Terms
10. Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy"
11. Institute Innovative Protection of DoD System Design and Operational Information
12. Institute Industry-Standard Information Technology (IT) Practices in all Software Developments
13. Require Vulnerability Monitoring, Coordinating, and Sharing across the Supply Chain of Command
14. Advocate for Tax Incentives and Private Insurance Initiatives
15. For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance

For the long term, DoD should articulate an end-state or strategic endpoint to serve as a "North Star" to guide and measure progress. We believe this initial collection of recommended actions within the *Deliver Uncompromised* framework is a solid foundation for this strategy.

Contents

Understanding the Scope of the Threat

The character of war is changing. Our adversaries no longer have to engage us kinetically; they have shifted their strategy to engage us as a nation *asymmetrically*, exploiting the seams of our democracy, authorities, and morals. They can respond to a kinetic action non-kinetically and often in misattributed ways through *blended operations* that take place through the supply chain, cyber domain, and human elements. They can render our national capability to project power—hard or soft—non-mission ready. They can collapse and even reverse the decision cycle.

> We are in an era of adversarial asymmetric warfare for which we have no comprehensive deterrence.

Nation-state adversaries have exploited cyber and supply chain vulnerabilities critical to U.S. security for hostile purposes. These include exfiltration of valuable technical data (a form of industrial espionage); attacks upon control systems used for critical infrastructure, manufacturing, and weapons systems; corruption of quality and assurance across a broad range of product types and categories; and manipulation of software to achieve unauthorized access to connected systems and to degrade the integrity of system operation.

The missions for which the Department of Defense (DoD) are responsible are particularly vulnerable. Adversaries seek to counter areas of U.S. military dominance and to challenge U.S. interests in cyber domains via supply chains upon which our government, our industries, and our populace rely. In this space, traditional boundaries of threat, action, and response are blurred. *We are in an era of adversarial asymmetric warfare for which we have no comprehensive deterrence.* The contemporary threat landscape has not been effectively addressed or deterred in our national security missions, policies, and infrastructures. The response is inadequate within the private sector and across government. The mission readiness of the U.S. military and its ability to project force are at grave risk. Our adversaries have developed and demonstrated capabilities to collect valuable intelligence on defense capabilities, steal intellectual property, initiate offensive action, and respond to provocation in an asymmetric manner. They target military as well as private sector U.S. interests, using means that make attribution problematic. These conditions are without precedent and threaten mission resilience and national security.

Our supply chains are exposed to multiple threat vectors. Supply chains are one of the four primary elements of an adversarial attack via blended operations. Attacks may be mounted against the entire supply chain life cycle from conception to retirement. The supply chain is vulnerable to adversary insertion of counterfeit parts that pass ordinary inspection but fail operationally. Largely through cyber-physical threats, adversaries may introduce malware or exploit latent vulnerabilities in firmware or software to produce adverse, unintended, and unexpected physical effects on connected

or controlled systems. Supply chains as a service present another critical exploitation vector.

MITRE initially launched this study to help DoD strategically address software supply chain challenges in light of recent legislative branch interest in how "software provenance" was being addressed after the recent Department of Homeland Security Binding Operational Directive 17-1 dealing with Kaspersky Laboratory software. To that end, the report has a pronounced emphasis on addressing software supply chain security. However, the impact of supply chains as a service, hardware, and software on DoD mission readiness and ability to project power requires a strategy that encompasses all aspects beyond just software and within software, beyond just concerns surrounding Kaspersky. To that end, in this report we define supply chain as:

> The system of organizations, people, activities, information, and resources involved from development to delivery of a product or service from a supplier to a customer. Supply chain "activities" or "operations" involve the transformation of raw materials, components, and intellectual property into a product to be delivered to the end customer and necessary coordination and collaboration with suppliers, intermediaries, and third-party service providers.

The resulting COAs should be considered in that light so that the resulting strategy addresses services and hardware in addition to software supply chains.

The result of these attacks is damage to U.S. military readiness, as well as the infrastructure and commercial systems upon which our military relies. Inadequate defense can nullify the value of government and private sector investment and erase expected benefits of new technology. Adversaries will mount cyber and supply chain attacks to slow the progress and deployment of new defense technologies, to compromise the operation and reliability of defense mission and business systems, to replicate what the U.S. technology base has accomplished, and to defeat or deny expected military advantages from U.S. investment in emerging technologies. Stronger, holistic measures to make our networks and supply chains more robust and resilient can deter adversaries by increasing the costs or even reversing the likelihood of adverse effects—reducing the "return on investment" of potential attacks. While one aspect of deterrence is the threat of retorsion or retaliation, a complementary aspect is "gain denial" through measures that deny adversaries confidence in successful attack.

Software vulnerability is a new dimension of security risk, as defined by threat, vulnerability, and consequence, that has received too little recognition. For many if not most DoD systems, software now defines function. Software increasingly determines the boundaries, operation, and risks to systems relied upon by all facets of civil society—consumer-facing, industrial, transportation, energy, healthcare, communications—as well as defense missions and management. Increasingly, functionality is achieved through software. A modern aircraft may have more than 10 million lines of code. The initial Block 1A/1B F-35 had more than 8.3 million lines of code, and later versions

of the aircraft will have more than 20 million lines of code for both operations and support. Combat systems of all types increasingly employ sensors, actuators, and software-activated control devices.

The proliferation of command-driven electronic systems, increasingly connected to sensor-informed networks (even if not initially designed for such linkages), massively expands opportunity for mischief or physical injury achieved through cyber-physical attacks. Software assurance needs to be made a priority for all phases of system acquisition and sustainment. DoD needs to work closely with technical community industrial partners to demonstrate and deploy new methods and measures to identify and respond to software vulnerabilities. Such initiatives acquire new urgency as more and more systems become interdependent and reliant upon the growing instrumentalities of the Internet of Things (IoT).

This report examines options that span legislation and regulation, policy and administration, acquisition and oversight, programs and technology. Actions are presented for the near, medium, and long terms—recognizing the need for immediate action coupled with a long-term commitment and strategy. Cyber and supply chain vulnerability extends well beyond DoD, across government and into the private sector. Nonetheless, DoD has potentially decisive influence in this space. DoD can implement policy and organizational changes, use its acquisition power, and manage the utilization of technology and research and development to address the problems. Beyond DoD, actions in the legislative domain are critical, as our adversaries are actively exploiting seams and shortcomings in areas such as information sharing, threat detection, and acquisition transparency. Building effective deterrence to asymmetric threats will require time and deliberate planning. For the long term, DoD should articulate an end-state or strategic endpoint to serve as a "North Star" to guide and measure progress. We believe this initial collection of recommended courses of action (COAs) within the *Deliver Uncompromised* framework is a solid foundation for this strategy.

Objective: Deliver Uncompromised and Resilient Systems

For the service components that ultimately own the responsibility to execute DoD mission and hence resilience, the primary goal of DoD must be to deliver warfighting capabilities to Operating Forces without their critical information and/or technology being wittingly or unwittingly lost, stolen, denied, degraded, or inappropriately given away or sold. The myriad of systems and capabilities that enable these missions must be resilient and able to respond to anticipated penetrations. The Department's acquisition mechanisms reward cost, schedule, and performance more than integrated risk-management upon which many capabilities rely, especially systems which depend upon complex software. For some years, the Department has pursued a succession of successful "Offset" strategies, focused on innovation in sensors and in network-centric warfare to produce advantages in the delivery and lethality of kinetic firepower. There has been no corresponding strategy, however, for securing that innovation from compromise with an emphasis on mission resiliency. Instead, all too often the Department and its contractors have used a lowest cost set of disparate, unsynchronized security activities and processes that do not match the importance of innovation, information, and technological superiority to our National Security Strategy, National Defense Strategy, and National Military Strategy. The objective of the *Deliver Uncompromised* strategy is to directly address this point, and institute a deliberate, inherent elevation of integrated risk management from concept through retirement, within the DoD and its contracting base, to ensure mission resilience. Choosing not to fight on our terms, our adversaries have embarked upon strategies that exploit the arbitrage of non-coherent defenses and rely on asymmetric capabilities to defeat our technological advances. As evidenced by all-too frequent media reports, our adversaries have had significant success in their strategy. Critical private-sector and military capabilities have been compromised through blended operation attacks, to one degree or another, at various points along the system development life cycle, sometimes prior to delivery, sometimes during sustainment.

State-of-the-Art Security

Independent analysis, respecting the skill and intention of adversaries in asymmetric warfare, should assume that the Department already has experienced systemic compromise, the impact of which may not now be knowable.

Independent analysis, respecting the skill and intention of adversaries in asymmetric warfare, should assume that DoD already has experienced systemic compromise, the impact of which may not now be knowable. The contemporary state of security, unique in the modern era, demands not an "improvement in the same" so much as

a "quantum change" from orthodoxy and established conventions. The response requires a number of strategic actions, some within DoD's span of control, such as leveraging technology and policy, and others, such as legislation or Executive Branch action, requiring the participation and leadership of Congress, the President, and other Executive Branch participants.

For the near term and beyond, the key operational imperative must be to obtain and maintain positive operational control over critical information and technology/capabilities. This imperative extends the benefit of *Deliver Uncompromised* from the acquisition community to the operational community, because maintaining positive operational control is a key element of planning, command assurance, mission execution, and sustainment. Essentially, every element's survival depends upon the ability to release, convey, or transfer information and/or technology under their own initiative and not the unapproved initiative of others. This key imperative may prove to be exceedingly difficult to achieve. DoD and its contractors will have to accept shared responsibility in which all participants take ownership of the challenge and assume a duty of continuing initiative. Absent such an approach, as a nation we risk dilution, or loss, of strategic and tactical advantages.

Too often the focus of government efforts to improve contractor cyber measures is upon perimeter defense, with security professionals assigned principal responsibility. The established presence of Advanced Persistent Threats (APTs) calls into question the operating premise of perimeter security. Counterintelligence personnel need to work with security professionals to inform enterprise actions with an understanding of adversary targets, methods, and priorities.[3]

Today our adversaries may have a better understanding of our strategic vulnerabilities than do we. This includes vulnerabilities introduced via networks or through the supply chain. This is because of poor/inadequate intelligence on such threats, excessive compartmentation that precludes effective sharing of such threat information, lack of prioritization, and widespread availability of information in the public domain. Combined with the inherent vulnerabilities of the natural seams of our democracy,

3 Experience has shown that external sensors for detecting network penetration do not reveal all attempts at penetrations or detect unauthorized outflow that results from APTs. In blended operations, adversaries may avoid the network perimeter and instead use tactics to attack supply chain hardware, software and services. George Patton's observation applies here for how France's Maginot Line, a static defense against German invasion, failed miserably. "Fixed fortifications are monuments to man's stupidity. If mountain ranges and oceans can be overcome, anything made by man can be overcome." The threat environment requires the United States to adopt a counterintelligence mindset to replace our legacy security mindset when securing the defense industrial base. Our adversaries' great success against static defenses should be evidence enough that we need to make this change. To win in the Information Age where the advantage is to the attacker and not the defender, our new frame of reference should be: 1) no defensive perimeter wall is inviolate; 2) every wall has been penetrated or is susceptible to successful penetration by determined actors; and 3) the absence of evidence our security wall has been breached does not constitute evidence there has been no penetration.

this gives our adversaries a significant advantage to which we are just beginning to respond.

The 2018 National Defense Strategy recognizes the degradation of our force projection capability across all domains and specifically calls for the investment of resilient capabilities:

> "Investments will prioritize ground, air, sea and space forces that can deploy, survive, operate, maneuver and regenerate in all domains while under attack. Transitioning from large, centralized, unhardened infrastructure to smaller, dispersed, resilient, adaptive basing that include active and passive defenses will also be prioritized." Likewise, "...New commercial technology will change society and, ultimately, the character of war. The fact that many technological developments will come from the commercial sector means that state competitors and non-state actors will also have access to them, a fact that risks eroding the conventional overmatch to which our Nation has grown accustomed. Maintaining the Department's technological advantage will require changes to industry culture, investment sources, and protection across the National Security Innovation Base...".

The recommended measures in this study are intended to serve as a foundation which directly supports this strategy.

Structural Challenges

There are fundamental structural challenges facing the Department. If not resolved, these barriers will undermine our ability to *Deliver Uncompromised*. Major challenges to consider are:

1. Overreliance on "trust," in dealing with contractors, vendors, and service providers, has encouraged a *compliance-oriented* approach to security—doing just enough to meet the "minimum" while doubting that sufficiency will ever be evaluated. This approach must change fundamentally so that enterprises are incentivized to find and solve any issue that might place a program at risk or expose systems to vulnerabilities. At the same time, industry needs the means to assess and validate their countermeasure accomplishments. We offer suggestions on how to establish an independent, expert intermediary that industry will trust to develop security metrics and necessary processes for review and assessment.
2. Solving the security issues facing DoD requires increased *counterintelligence* (CI) participation. A *security* community that largely operates to show compliance with established rules may be uninformed of evolving threats and therefore unable to adapt to the agile strategies and asymmetric techniques of adversaries. From Defense Security Service (DSS) reports and supporting documentation by the National Counterintelligence and Security Center (NCSC), as well as

Federal Bureau of Investigation (FBI) field office activities, there are lessons to be learned from the resources that are actively engaged in CI activities. Protection of DoD interests calls for Department leadership, as well as industry, to be kept alert and informed, by DSS, the FBI, and other entities, about the quiet attacks constantly being launched against DoD interests. This is why education and ownership of the problem are so important—and why expanding the resources and authority of DSS is vital.

3. There is no single DoD organization vested with lead responsibility for threats and risks to the defense industrial base (DIB), despite the fact that most major exploitations by adversaries are directed against and occur within the DIB. DoD should consider the DIB assets on a "whole of enterprise" basis, inclusive of assets beyond information and data, and shift from protecting *facilities* to protecting *assets*. Similarly, DoD's contract measures, and accompanying oversight, should evolve from safeguarding *information* and *information systems* to include safeguarding *operations* and enterprise *capabilities*. In this vein, the Department should address its interface with contractors for security practices, so that companies deal with trained resources and avoid inconsistent interpretations and instructions.

4. There has long been widespread recognition that "reform" of the existing acquisition process is needed to address typically over complex, behind schedule, and over budget acquisitions. However, given the changing character of war and our adversaries' asymmetric strategies, these processes, along with how we have maintained and sustained our capabilities, have also resulted in highly compromised systems despite the consumption of huge technical and financial resources, leaving the Department's mission readiness at risk. This fact must drive true reform of the acquisition process. The Vice Chiefs and the Vice Chair, who are ultimately responsible for the operational readiness for their Services, should create and maintain a strong and accountable chain of command for cyber defenses, supply chain security, and digital integrity, and themselves be held accountable. Accountability for integrity and mission readiness must be blended across the acquisition, operations, and sustainment communities, with a clear chain of command directly to the Secretary of Defense (SECDEF) through the Deputy Secretary of Defense (DEPSECDEF).

5. DoD (among other federal departments and agencies) has yet to communicate clearly with sufficient emphasis the importance of security and integrity. This failure is reflected in the recently released *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018). Across the entire range of enterprise, business, and weapons systems, the Department will benefit from a clear leadership statement and direction that shifts priorities and reduces exposure to compromised delivery. At the national level, the Office of Management and Budget's (OMB) Memorandum M16-04, "Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government," dated Oct. 30, 2015, included

directions to the heads of executive departments and agencies that still merit attention today. Agencies were directed to prioritize identification and protection of high-value information and assets, improve ability to timely detect and rapidly respond to cyber incidents, prepare for rapid recovery from incidents when they occur, recruit and retain the most highly qualified cybersecurity workforce, and make efficient and effective acquisition and deployment of both existing and emerging technology.

Contractual Leverage

Ultimately, improved cyber and supply chain security requires a combination of actions on the part of the Department and the companies with which it does business. Through the acquisition process, DoD can influence and shape the conduct of its suppliers. It can define requirements to incorporate new security measures, reward superior security measures in the source selection process, include contract terms that impose security obligations, and use contractual oversight to monitor contractor accomplishments. There are limitations upon what DoD can accomplish. DoD is not so large a customer that it can control all parts of the supplier base upon which it draws. And DoD has strongest influence over companies (large and small) with which it contracts directly. Nonetheless, DoD spending is a principal source of business for thousands of companies. The Department can reward the achievement, demonstration, and sustainment of cyber and supply chain security. It will take time to establish workable, fair processes, but these efforts should be given high priority. Where justified by urgent circumstances, the Department should consider use of interim rules to effectuate DU in near-term procurements. Adding more security measures to the "acquisition toolkit," and making better use of those measures, are ways DoD can exercise security leadership through use of its contractual leverage. This issue is elaborated more fully in *Annex I* of this report.

Courses of Action (COAs)

To succeed with *Deliver Uncompromised* requires commitment at the *enterprise* rather than the *element* level—for the Department and for its contractor base. Given the threat environment and its consequences for DoD, this report identifies a number of strategic elements—courses of action (COAs)—to address the cyber and supply chain security challenge. We classify actions into short term (ST), medium term (MT), and long term (LT), based on how quickly and urgently the Department should *initiate* action. The COAs are listed here and described in more detail further in the report:

COAs		
1	Elevate Security as a Primary Metric in DoD Acquisition and Sustainment ST	It is vital to *Deliver Uncompromised* that security have equal status to cost, schedule and performance. Revise DoD 5000.02 and Defense Acquisition Guidance to make security the "4th Pillar" of acquisition planning, equal in emphasis to cost, schedule and performance. Utilize acquisition tools and contract leverage and reinforce the objective of *Deliver Uncompromised* through the use of positive and negative incentives.
2	Form a Whole of Government National Supply Chain Intelligence Center (NSIC) ST	Follow the example of the National Counterterrorism Center (NCTC) to integrate Title 10 and Title 50 "all source" supply chain threat intelligence and strategic warning. Led by NCSC and heavily supported by an expanded DSS capability, extend out to include FBI, DHS, and other civilian agencies and share warnings and actions with contractors.
3	Execute a Campaign for Education, Awareness, & Ownership of Risk ST	Educate all program and supply chain participants of the goals of *Deliver Uncompromised* and the breadth and nature of cyber and supply chain threats. Build and maintain training programs for DoD personnel, including measures to improve the expertise of persons assigned contractor oversight responsibilities.
4	Identify and Empower a Chain of Command for Supply Chain with Accountability for Security and Integrity to DEPSECDEF ST	The Service Vice Chiefs are ultimately responsible for the operational readiness for acquired capabilities under their command and should require that acquisitions are conducted in a manner that values system integrity and mission resilience to *Deliver Uncompromised*. Cross-Service vulnerabilities and opportunities for effective threat response across the Department can be served by the Vice Chairman, Joint Staff, and possibly an accountable Supply Chain Security Executive. Organize resources to support this chain of command and hold them accountable to the DEPSECDEF for successful implementation.
5	Centralize SCRM-TAC with the Industrial Security/CI mission owner under DSS and Extend DSS Authority ST	The Supply Chain Risk Management – Threat Analysis Cell (SCRM-TAC) is isolated from industry information sources and from operational elements supporting industry that are vital to structured SCRM analytic production. DSS has access to DIB information on classified contracts and has operational elements directly supporting industry. Consolidation could significantly improve DoD's cyber and supply chain strategic warning. This consolidation would result in a well-staffed and organized body of independent analysts, well trained in structured analytical techniques, which then could be positioned to help the program acquisition community directly address risk to programs as a function of not only threat, but system vulnerabilities and potential consequences.

COAs		
6	Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations ST	Ensure that the entire DoD leadership is aware of the goal of DU and that adversaries seek not to engage the United States kinetically but instead are using cyber and supply chain attacks to exploit and degrade key national security capabilities. Educate leadership in DoD to "own" the problem and make detection and defense against these threats a natural part of everyday duties.
7	Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software MT	Develop, validate, and exploit technical methods to assess and validate software security and integrity. Evaluate whether to require suppliers to use independent continuous monitoring to detect software nonconformity and developmental abnormalities and to automate patching and recovery.
8	Advocate for Litigation Reform and Liability Protection MT	Reduce liability exposure to encourage prompt contractor reporting of cyber and supply chain events. Encourage investment in integrity measures by providing new liability protection (e.g., extend SAFETY Act to cyber and supply chain).
9	Ensure Supplier Security and Use Contract Terms MT	In new acquisitions, treat data security, product integrity, and supply chain assurance measures as competitive discriminators, and make end-product mission resilience a key contract award metric. Consider use of interim rules to expedite the availability of these tools for critical near-term procurements. Structure acquisitions so contractors have a profit motive to enhance security; establish standards and methods to enable contractors to earn and retain levels of independently verified established resilience. Use an independent Security Integrity Score (SIS), much like a "Moody's" rating in the financial world, which rates each potential contractor in a unified manner by an independent, unbiased third-party.
10	Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy" MT	Extend existing authority to protect DoD against risks of contracting with entities under control of adversaries; provide for expedited action in high-threat situations. Empower the Supply Chain Executive to act on NSIC advice in conjunction with enforced responsibilities within the Combatant Commands against awards to sources of established assurance risk.

COAs		
11	Institute Innovative Protection of DoD System Design and Operational Information MT	Minimize and obscure the dissemination of system design information, even within the design and build teams, but especially with vendors and contractors. Share what information needs to be shared only as long as needed and no more; utilize technical measures to protect data access and use rights at the file level.
12	Institute Industry-Standard Information Technology (IT) Practices in all Software Developments MT	Address the full span of software vulnerability through measures in acquisition and operations through full life cycle continuous security and risk reduction practices from concept through retirement. Determine where and for what programs or missions it is recommended or necessary to require submission of a Software Bill of Materials (SBOM) and require a documented Secure Software Design Life Cycle (SSDL).
13	Require Vulnerability Monitoring, Coordinating, and Sharing across the Supply Chain of Command MT	The NSIC should serve as the focal point to aggregate vulnerability information across all sources of public and private source information, including Defense intelligence and other IC content. Each Service component in both acquisition and sustainment should look for and coordinate information sharing among themselves and with designated software vulnerability information sharing mechanisms such as Common Vulnerabilities and Exposures (CVE), Information Sharing and Analysis Organizations (ISAOs), United States Computer Emergency Readiness Team (US-CERT), National Telecommunications and Information Administration (NTIA), and Department of Justice (DOJ).
14	Advocate for Tax Incentives and Private Insurance Initiatives LT	Work with Congress to provide tax incentives for contractors that invest in cyber and supply chain assurance, which is independently and routinely evaluated. Promote contractor use of cyber and supply chain insurance with government excess liability coverage.
15	For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance LT	For every critical function for which the consequence of an attack is denial of mission execution, develop means to execute the mission in a degraded state while under attack. Utilize "uncorrelated means" of accomplishing the missions in system and subsystem designs and diversity at the component, Service, or enterprise levels.

COA Details

1. Elevate Security as a Primary Metric in DoD Acquisition and Sustainment (ST).

Acquisition today is driven to meet cost, schedule, and performance objectives. Absence of incentives for security contributes to widespread compromised systems. Currently, the misalignment of risk and reward during acquisition results in systemic risks being transferred to the operational and sustainment communities without accountability. DoD must shift from measuring program progress primarily by financial considerations to a metric of durable operational readiness of acquired systems. Planning must account for the true cost of ownership of capabilities. Existing contract authorities should be leveraged to require demonstration of system integrity and mission assurance to be a deliverable, to the best extent reasonably possible; software security and system resilience should be Key Performance Parameters for contract execution. Methods of providing continuous monitoring of system integrity and having alternate means of executing mission function through system design and engineering (at the subsystem, system, and enterprise levels) and through prepared operational strategies are essential to increasing resilience and "fight through" capability.

As we introduce new and more secure processes to the private and public sectors, increased cost is to be expected. Absent adjustment, cost factors too often drive decision making away from the desired security outcome. When viewed from the asymmetric threat perspective, this is an undesirable outcome that can be avoided only through high-level priority, policy, and accountability changes. Part of the new strategy must be to transform security concerns from a cost center to a profit center. Additional funding will be needed to avoid the outcome that treating security as a "4th pillar" will produce undesirable compromises to cost, schedule, or performance. Products free of compromise represent more value than compromised products and have reduced total cost of ownership.

Means of accomplishing this objective are further discussed in this report. One important strategy is to use acquisition authority to adjust the expectations of private sector contracting partners. Few DIB participants disagree that a better job can be done with security and integrity. Many, however, are unsure how to "benchmark" what they have accomplished so as to manage their own progress and, if asked, demonstrate to DoD, or to primes or higher tier contractors, that they are worthy of trust.

To realize security as the "4th pillar" requires that the degree of risk a current or potential contractor presents to the government be continuously measured and monitored. We see this evaluation taking place in three dimensions: measured by the government on currently performing contractors as a future performance indicator; measured by an independent not-for-profit or federally funded research and development

center (FFRDC) much like a "Moody's" score and made publicly available; measured privately by the contractor via the private sector to monitor their operational risk.

The commercial sector is currently developing various services to address the last measurement technique. In investigating the second "Moody's"-like scoring, we have received a positive response, within the Department and DIB community, to creation of an independent, expert resource to create and operate a security scoring mechanism. Conceptually, SIS could be used in bidder qualification and in the selection and award of contracts. DoD and industry should partner to create an independently administered entity, perhaps a not-for-profit 501(c)(3) organization, to create standards and processes for risk-based evaluation and scoring of contractors, perhaps separating contractors into "tiers" of accomplishment, and accompanied by commitments to continuous monitoring, reporting, and self-improvement. Use of SIS would be phased in, figuring initially into acquisition decisions for Major Defense Acquisition Programs (MDAPs) and other, selected high-impact programs. Over time, as government and industry become confident in the value of SIS, they can become an important part of the acquisition process for more programs and for many levels of the supply chain. Receipt of SIS credentials could be valuable in qualification for commercial supply chain participation as well.

All too often today, DIB contractors are reluctant to price added integrity and integrated risk management into their bids because the U.S. government rarely requires it in the Request for Proposal (RFP), and they fear losing the contract where higher cost may be a decisive negative discriminator. Adding security credentials into the mix by crediting SIS as earned should motivate contractors to make the needed investments and to secure development environments, moving security from the loss column to the profit column.

The historical emphasis on "cost, schedule, and performance" is a fundamental driver for actions of DoD as well as the DIB. The DoD requirements process has not put security and integrity on an equal footing, with the result that the costs of assurance work against the usual program metrics. This approach works against the integrity of weapon platforms in today's world of diverse and severe cyber and supply chain threats. For all aspects of the system development life cycle, and throughout operation, sustainment, and system disposition, security must have higher priority. Dispersed, agile, and evolving threats require continuous commitment from both government and industry participants. Special attention is required for software security—an area of great exposure but given relatively low priority at present.

Even after increasing the importance of security across the acquisition process, there are other areas DoD needs to address for continuous improvement over a longer term:

- The Department already invests in new technologies that can be applied to identify and mitigate cyber and supply chain threats in the near term, mid-term, and long term. Where breakthrough technologies are found, they should be rapidly

exploited. The Department already is expanding use of non-procurement "Other Transaction Agreements" (OTAs) under 10 USC §2371b. To encourage innovation by its established and dedicated contractors, the Department should be able to make OTA awards to both "nontraditional" and "traditional" defense contractors. Beyond application to prototype projects, DoD may need clarified and enhanced legislative authority for transition from prototype to production and deployment, where justified by national security considerations.

- Constraints remain in the ordinary application of today's "full and fair competition" rules to DoD acquisition at all phases of the system life cycle. Further study is needed to remove barriers to rapid, secure accomplishment of national security goals, while recognizing that competitive opportunity encourages industry participation and innovation. In the same vein, the Department should consider whether pending "acquisition reform" initiatives (such as the Section 809 Commission) give sufficient weight to security. As it considers the 809 Commission recommendations, the Department must assess the tension between current and planned reform actions and the full scope of the asymmetric threat and response.
- DoD needs to retain the trust of its contractors, who will not invest as needed in security (or in new technologies) without assurance of opportunity for return through a fair competitive process. Program budgets must incorporate funds sufficient for higher levels of security. Product integrity, data security, and supply chain assurance should become key contract award criteria. This will remove today's security disincentive, as contractors now risk the award should they include costs that ensure delivery of uncompromised capabilities. In the competitive source selection process, DoD should incentivize bidders to make demonstrable and independently verifiable improvements to the protection of their system development and delivery processes and to sustained security over system life.
- "Transparency" and "open government" have policy benefits but expose massive amounts of exploitable information to adversaries, contributing to their knowledge base without counterpart exposure to the United States. This must stop. For high-impact programs and critical technologies, and in areas where known cyber and supply chain risk is present, the Department may need authority to obfuscate program and procurement information—and it will need corresponding capabilities from its private sector partners and their suppliers.
- DoD has reasons to seek more knowledge of contractor technologies, more data about as-built configurations, and more insight into supplier selection, pedigree, and provenance. These interests must be balanced with recognition that intellectual property (IP) is a critically important asset to many contractors, and DoD must assure its suppliers it can protect their IP, where demanded and delivered, and that contractors will retain the ability to exploit the IP of their innovations. DoD should always be mindful that its contractors must have a positive business case before they incur new costs and responsibility for software assurance or other security improvements.

Deliver Uncompromised

For budgeting and planning, the Department needs to address the financial consequence of losing or utilizing a compromised critical system—including the ultimate cost of a failed mission for which the capability was developed in the first place. Likewise, much of the technological advantage the United States has enjoyed is constantly eroded due to adversary theft of key designs and technologies. (There are numerous examples of nearly identical adversary capabilities that our enemies have fielded as a result of compromised acquisitions.) To provide the requisite system security or confidence—from the outset rather than as a midlife correction or enhancement—realistic resource assessments should be factored into the expected acquisition and sustainment budgets. As shown in Figure 1, the up-front costs of a representative acquisition appear significantly different for a supply chain adequately protected from inception. The apparent cost differential, however, is significantly smaller for the protected acquisition when compared to the higher total cost of ownership experienced where failure to secure the supply chain initially delivers compromised products requiring expensive attempts at correction later in program life.

Once an exploited vulnerability is discovered, a new acquisition effort will be required to replace or re-engineer a deployed system. If the process is not protected, it may be

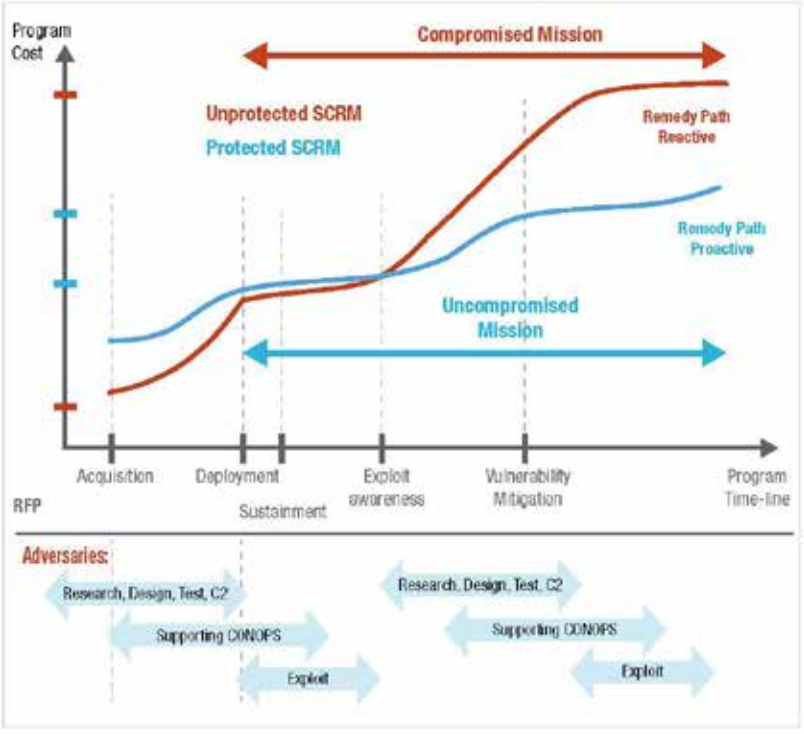

Figure 1: Cost framework for SCRM: Total cost of ownership implications

attacked again. Most serious in this entire paradigm is the loss of the ability to ensure that the mission for which the system is designed can be successfully conducted, and/or the loss of overmatch of the U.S. capability over the adversary.

2. Form a Whole-of-Government National Supply Chain Intelligence Center (NSIC) (ST).

Supply chain threats include but extend beyond the DIB. A whole-of-government (WOG) response first includes DoD and the IC with likely leadership from the National Counterintelligence Security Center (NCSC). This strategy then should then be extended to FBI, DHS, and other civilian agencies. DoD should endorse and support a national joint, inter-agency entity—the NSIC—that can aggregate all-source data, both classified and unclassified, cyber and non-cyber, and share it with at-risk operators and industrial partners. The NSIC should follow the NCTC model functionally. The NSIC would be jointly governed, likely reporting to the Director of National Intelligence (DNI), the Under Secretary of Defense for Intelligence (USD[I]), and the NCSC. The goal of the NSIC would be to support the delivery to Operating Forces of warfighting capabilities that are uncompromised and resilient (i.e., without their being wittingly or unwittingly lost, stolen, sold, inappropriately given away, degraded, or denied) through the use of all-source intelligence and warning. In the wake of the 9/11 events, President Bush worked with Congress to create the NCTC to enable the responsible exercise of new investigative and analytical authorities and information collection, consolidate data, facilitate information sharing, and provide national, state, and local warning within and across various public-sector entities. Its stated purpose is to "lead and integrate the national counterterrorism (CT) effort by fusing foreign and domestic CT information, providing terrorism analysis, sharing information with partners across the CT enterprise, and driving whole-of-government action to secure our national CT objectives." Creation of the NSIC would be a similar initiative, drawing from experience and lessons learned over more than a decade of NCTC operations. From the DoD perspective, this could be partially realized by centralizing SCRM-TAC with the Industrial Security/CI mission owner under DSS lead.

With new authorities supported by policy and legislative changes, the NSIC would be able to share intelligence-based strategic warning among all DoD components and mission owners and, eventually, with all U.S. government (USG) department and agencies. This would contribute to a national resource for threat collection and analysis that produces actionable intelligence and measures that can be utilized across the WOG at the unclassified level. This integrated resource would develop and operate technologies for threat detection, artificial intelligence, and data analytics, enabling analysts to "connect the dots" among subtle and disparate data from a wide variety of sources. Risk assessments require an understanding of system vulnerabilities and their consequences across the supply chain cycle, as shown in Figure 2.

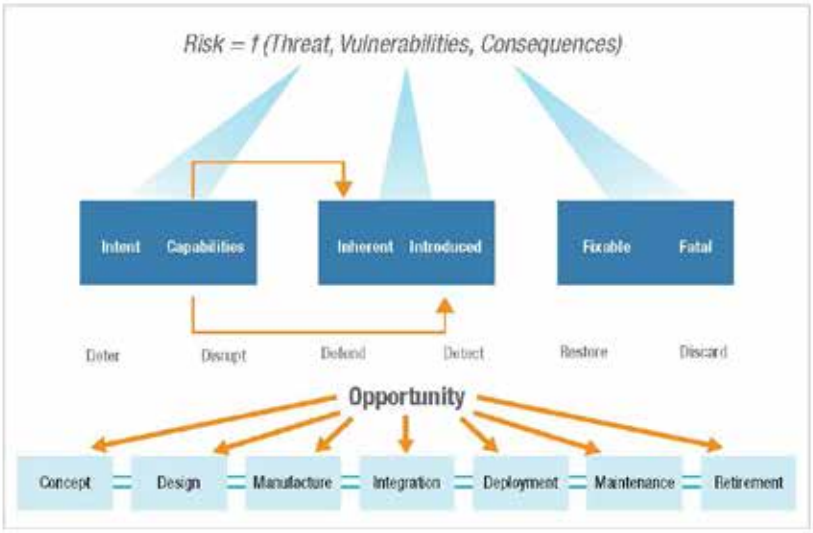

Figure 2: Supply chain risk assessment and integrated response

Risk assessment is crucial to supply chain defense and assurance of system integrity. Knowing the threat is the essential first function of successful risk assessment and supply chain defense. Existing stovepipes of legacy sectoral assignments hinder fully informed actions. Imperfect or incomplete intelligence dilutes the value of assessments and recommended actions while increasing the probability of a missed detection or false alarm. The NSIC will generate high-value threat assessments and be positioned, through joint interagency interactions, to help its component members develop measures of risk based on their specific vulnerabilities and mission failure consequences. It can combine all-source government intelligence, data from civilian agencies, and private sector reports.

As the center of excellence for supply chain strategic warning and risk assessment, the NSIC will be expert in knowing potential system vulnerabilities (inherent or introduced) if populated with representatives from the program and system engineering communities. The NSIC should be staffed with and led by trained analysts and subject matter experts who understand both the engineering technical characteristics of a potential exploitation as well as potential tactics, techniques, and procedures (TTPs) an adversary may use. Multiple, diverse stakeholders from across the development and acquisition community can use warnings produced by the NSIC. Consequences can be averted or mitigated by timely warning coupled with expert advice on response and recovery, as shown in Figure 3.

Attention must be directed to communicating strategic warnings (and action recommendations) to industry, as it is frequently the target and is best able to protect.

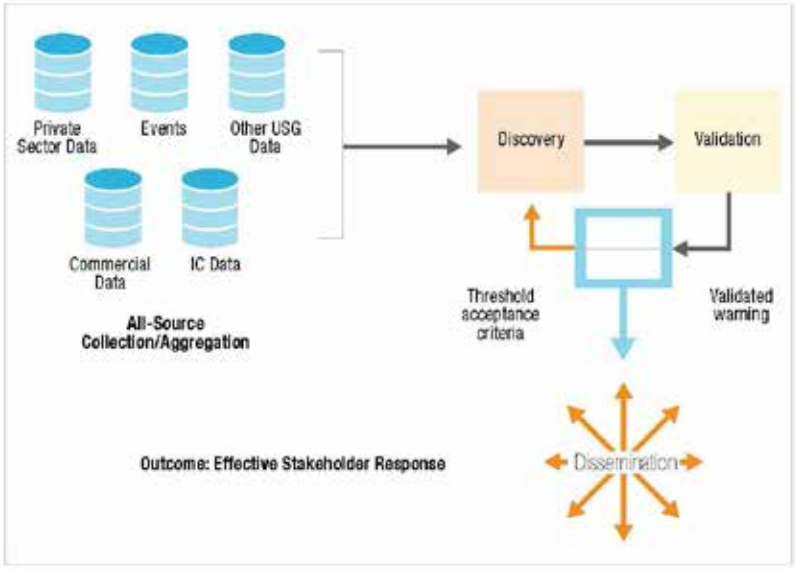

Figure 3: Distribution of source data, validation and warning, and action

detect, respond, and recover. Today, the distribution of threat information to industry—if it occurs at all—is too slow and too cumbersome. In an information age, means are needed to communicate electronically to industry. Methods must be established to share threat information and recommendations with companies who are not cleared contractors. It is difficult to translate from classified threat data into unclassified warning, but this is a responsibility that should be assigned to the NSIC. Informing only cleared industry is not satisfactory—it leaves the great majority of companies in the DIB uninformed and exposed.

This concept can also significantly reduce duplicative government purchasing of commercial data sources.

3 Execute a Campaign for Education, Awareness, and Ownership of Supply Chain and Digital Risk (ST).

Program executives and the acquisition workforce must be better informed, educated, and trained. The entire acquisition and sustainment community must become aware of the expanse of the asymmetric threat we face. As a matter of duty, supporting personnel must understand and "own" the problem—namely a lack of appreciation of how the new threat environment has made the supply chain a vector of attack and that this vulnerability continues for the entire supply chain cycle. As stated at

the outset, the supply chain is exposed to multiple threat vectors and categories. As shown by the recent experience with Kaspersky Labs anti-virus software, our software supply chains are being exploited, potentially on a massive scale, that could produce a host of nefarious outcomes. Supply chain risks extend beyond the subject of cybersecurity that often dominates the attention of Department leadership. Risks exist through the entire supply chain cycle and are not limited to networks and information systems. Deliberate insertion of non-conforming parts can sabotage mission capability. The firmware or software in electronic parts can be the subject of corruption or subversion. Adversaries, unfortunately, have many choices among attack surfaces to produce effects adverse to defense planning and mission execution.

New comprehensive curriculums on supply chain risk and asymmetric adversary intent should be readily available at the Department (e.g., Defense Acquisition University, National Defense University, National Intelligence University, etc.) and Component levels to members of the acquisition, operations, and sustainment communities.

The human factor contributes to supply chain risk. Individuals can enable, even engineer, hardware and software attacks. Insider threats remain among the most important causes of successful compromise. They can arise by design and intention, where an insider is untrustworthy, subject to foreign control or influence, or otherwise suborned, through means such as a social engineering attack. The same outcome can result from imprudent or uninformed actions without any hostile intent, by persons who lack sufficient training or who are given unmonitored or overbroad access to or authority over connected systems. Best practices for supply chain protection, in government and industry, call for improved training and better monitoring to detect, limit, or prevent insider-caused events.

Too often, within DoD and industry, senior executives pay insufficient attention to supply chain assurance—and too little investment of money or other resources—because they lack sufficient understanding of the problem and the hidden operational risks they incur. The awareness campaign recommended here is not a one-time or static exercise. Training has to evolve to keep pace with the intense rate of change in this threat/response landscape.

4. Identify and Empower a Chain of Command for Supply Chain with Accountability for Integrity to DEPSECDEF (ST).

How systems are engineered and designed in the future should be a fundamental focus for the Defense Research and Engineering (R&E) and Acquisition and Sustainment (A&S) communities. How capabilities are acquired and operated in a secure manner ultimately lies with those charged to organize, train, equip, and command—the Components. This needs to be reinforced. Consequently, the Service Vice Chief would be the official best positioned to reconcile inputs from Acquisition (cost, schedule and performance) and from the IC and CI (Security) through their development and approval of requirements and acceptance of delivered capabilities. Since supply chain security is an overarching domain—affecting requirements, acquisition, operations, and sustainment—the Service Component Vice Chiefs should own the responsibility to ensure that the acquisitions under their command and for their operations are conducted in a manner that values system integrity and mission assurance to *Deliver Uncompromised*. Cross-Service vulnerabilities and opportunities for effective threat response across the Department can be served by the Vice Chairman, Joint Staff, and possibly an accountable Supply Chain Integrity Executive within the Office of the Secretary of Defense (OSD). These resources should be organized to support this chain of command and be held accountable at the Vice Chairman and the Executive levels to the DEPSECDEF for successful implementation with authorities that span the Department.

Breadth of the Supply Chain Threat

Counterintelligence and security should not be subordinate to business and engineering professionals. The supply chain threat is larger than information and communications technology and extends beyond network-delivered cyber attacks upon information and information systems.

This authority should be coupled with personal accountability. The function affects all Military Departments as well as the fourth estate supporting agencies. Just as the corporate world is now standing up Vice Presidents for Supply Chain, and DNI/NCSC has a Supply Chain Directorate, DoD's supply chain responsibilities should be vested in these single individuals and offices with expanded authority and strong lines of interaction across the Department. Counterintelligence and security should not be subordinate to business and engineering professionals. The supply chain threat is larger than information and communications technology and extends beyond network-delivered cyber-attacks upon information and information systems. Accordingly, if system and supply chain integrity is viewed as its own mission, there are many contributing functions, among them Chief Intelligence Officer and cyber, CI and Defense Procurement and Acquisition Policy (DPAP), systems engineering and industrial base, etc. Considered as a whole, the potential function of a DoD supply chain executive reaches to

issues of technology base and national assets, such as foundries and field-programmable gate array (FPGA) assurance and supply, and the advancement of specialized assurance technologies such as automated software verification and emerging methods of authentication and measurement to protect against threat vectors from the IoT. Consolidated authority is needed for effective coordination among many contributing functions and to enable DoD *leadership* to make *strategic* decisions on approach, investment, and execution of assurance measures and to interact, coordinate, and collaborate across the WOG in a more consistent manner. It would ensure proper, accountable representations across the WOG as the nation begins to seriously deal with the supply chain security issue.

5. Centralize SCRM-TAC under DSS and Extend DSS Authority (ST).

SCRM-TAC, at present, is not well linked to USG and DoD assets performing operational intelligence, counterintelligence, security, and law enforcement prosecution. Although DoD, pursuant to instructions 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), and Committee on National Security Systems Directive 505, Supply Chain Risk Management, has worked with SCRM-TAC, Joint Acquisition and Protection Cell, and Joint Federated Assurance Center to produce a TSN Mitigation Playbook, vulnerabilities have continued to plague the process. SCRM-TAC focuses on portions of the *intent* and *capability* of adversaries, but not Component capability *vulnerabilities* and *consequences*, which are the domain of the acquisition and sustainment communities and elements of "DSS In Transition" currently being stood up. SCRM-TAC also is isolated from industry information sources.

DSS, in contrast, has CI operators in the field, and access to DIB information on classified contracts. The capability of DSS would be more robust and scalable if SCRM-TAC were to report to DSS. In this context, "report" should be understood to mean both administrative control and operational control. Production of supply chain intelligence would be enriched and accelerated by this change and further enhanced by combining these sources with content from the FBI and other authorities as needed. These would be initial steps for the Department's participation in a wider community-wide strategic warning capability, as is the intent of NSIC as described above. A consolidated, well-staffed and organized body of analysts well trained in structured analytical techniques could then be positioned to help program acquisition and sustainment to actually address *risk* to the program as a function of not only threat, but system vulnerabilities and potential consequences.

Elements of the acquisition community within DoD, however, are attempting to use SCRM-TAC as a clearinghouse on risk—a function that cannot be provided in the construct as described above. There are many elements and definitions of risk, and DoD should standardize on its own Defense Science Board and NCSC definition, as

illustrated in Figure 2 above. In some instances, SCRM-TAC is asked to provide the "risk" of a program utilizing specific components; in others, the risk of an entire system design. In nearly all instances, SCRM-TAC is utilized relatively late in the process, well after major procurement and design decisions have been made, and lacks sufficient information to conduct such assessments. At the program acquisition planning level, there seems to be less than recommended receptivity for strategic warning, especially when related to enterprise-wide threats. We have made several recommendations to specifically address these problems and approach supply chain security with threat analysis, information sharing, and intelligence management functions that would holistically address the challenge and mitigate risk. Although a daunting challenge, this report concludes that it is vital to recognize and address supply chain threats early in the acquisition planning rather than react later in the program cycle and attempt remediation after systems are built and deployed.

6. Increase DoD Leadership Recognition and Awareness of Asymmetric Warfare via Blended Operations (ST).

Our adversaries have demonstrated they wish to engage us *not* kinetically but rather asymmetrically. The landscape of potential non-kinetic adversary attacks is broad indeed. The United States lacks a comprehensive deterrence against these actions. We worry and debate over the possibility of a lawsuit by a contractor or supplier who is intentionally jeopardizing mission assurance while China openly discusses "lawfare" as a *strategy*. All levels of DoD leadership must fully understand the adversary's strategic intent to act through *all of* the supply chain (hardware, software, and service), cyber IT, cyber-physical, and the human element (witting or unwitting), and adjust the Department's response and posture accordingly.

As with other military domains (air, sea, land, and cyber), asymmetric warfare is, among other characteristics, complex and destructive, with offensive and defensive capabilities and a commitment to action (strategies and tactics). National leadership must recognize that we are currently in a state of war within all of these domains via asymmetric actions. The ability to take a whole-of-government or whole-of-society approach to combat an adversary's attack must take on the same level of investment, planning, and implementation we would exercise for a more conventional attack on our homeland and allies. A key part of the strategy is to reform our acquisition policies and authorities to combat an adversarial manipulation of the supply chain and work with the private sector.

The impact of this insidious asymmetric warfare against the United States has gone largely unrecognized. Some refer to this domain as conflict in the "gray zone" because of its comparative absence of visibility and the continuing challenge to attribution to responsible actors. Awareness of the true complexity of the asymmetric threat is distorted by the very nature of the technical and operational approaches our adversaries are employing in their attacks. Our response has been stunted because

of the lack of public awareness and understanding of adversaries' intentions, capabilities, or hostile acts.

Most nation-states have a full complement of technologies available to achieve their asymmetric strategies and goals. The development of effective approaches to take advantage of inherent vulnerabilities in complex systems is well within their capabilities and the access to our systems they enjoy through our supply chains. Likewise, through reverse engineering of complex systems, nation-states are capable of introducing or inserting vulnerabilities for exploitation.

This full-spectrum threat is not only capable of developing technical products, but is coupled with the requisite operational tradecraft, training, access development, and resources to mount an effective attack. All levels of DoD leadership must fully understand the adversary's strategic intent to act through blended operations.

Even the relatively unsophisticated actors, with limited or incomplete knowledge of our systems, can develop capabilities that have a profound impact on our offensive and defensive capabilities and infrastructures; to deny us the ability to effectively utilize them to achieve our tactical and strategic objectives. These capabilities are often available through third-party venues that leverage nation-state investments, often at low cost.

A significant shortfall in our defense is the lack of visibility to identify our adversaries' signatures or implementation across multiple domains and critical infrastructures. Indeed, misattribution of their actions is an important part of their strategy. In part this is due to the segmentation of responsibility we have imposed on ourselves for decades. Today, responsibility for risk to DoD capabilities is dispersed across departments and agencies and among many DoD Components and entities. The result is that leadership views their roles and responsibilities, with respect to security and acquisition integrity, through many different lenses. Each lens provides a limited view of the complete landscape in which we procure and maintain our weapon systems, exercise command and control, and utilize various infrastructures. A comprehensive, seamless approach is required to provide the requisite awareness, support, and *response of all participants* throughout the WOG enterprise.

As it is for other warfare domains, it is essential that an integrated approach to an education program, tailored for the various levels of participants from senior leadership through subject matter experts, provide a complete awareness of current procurement requirements and processes, the availability and utilization of intelligence, adversary TTPs, and the fundamental construct of adequate risk assessments and mitigation.

In the near term, we need to better utilize or leverage current authorities of departments, institutions, organizations, and agencies, and re-establish or confirm their roles and responsibilities, with the goal of reducing overall administrative burden,

redundancies, and costs, while vastly improving their effectiveness to combat asymmetric threats.

7. Establish Independently Implemented Automated Assessment and Continuous Monitoring of DIB Software (MT).

Mission-critical systems depend upon complex software assemblies with imperfect assurance. Where DoD programs require the DIB to develop custom software or exploit commercial and open-source software, DoD should require the application of automated validation tools and subject software to independent continuous monitoring for nefarious behavior. Independent validation is especially important where DIB primary and subcontractors use agile or DevOps environments. This may require the creation of a new, independent organization to evaluate the inherent risk within applications and processes, but this is already beginning to happen in the private sector. Ideally, this service should be provided by an independent, unbiased organization such as a not-for-profit or FFRDC. Preliminary conversations indicate that industry is more likely to embrace an assessment or credentialing organization if it is independent of government, though it also must have strong ties to government and the ability to receive and act upon information unique to government sources, including classified information.

Software security is a special risk. Some say, "software is the new hardware" or "software is everything." Software developers rely increasingly upon third-party components for today's complex applications. Much of the software used in devices and systems across all technology types is from multiple sources about which, in all but exceptional cases, little is known. Should adversaries insert malicious functionality into open-source components of software code or exploit latent vulnerabilities, the resulting corruption of the software tool chain can have pervasive and durable effects; these may not result in immediate harm but can be activated at the time chosen by an adversary. Hence, static assessment or static certification by itself is insufficient to ensure protection.

8. Advocate for Litigation Reform and Liability Protection (MT).

For DoD (and the WOG) to achieve and sustain cyber defense and supply chain resilience, government and industry must work together. Government laws and regulations can shape desired industrial behavior. Litigation and potential legal liability also figure prominently as both incentives and constraints on the way industry accomplishes security objectives. This is especially true in the production of software. DoD can lead efforts at litigation reform to manage liability risks and therefore to encourage positive industry behavior and facilitate timely government actions. This subject is addressed in *Annex II*.

9. Ensure Supplier Security and Use Contract Terms (MT).

Industry plays a crucial role. While DoD funds programs, conducts acquisition, and exercises oversight, it relies on the innovation and resources of its industrial base to execute programs and for the technological advantages our warfighters need. Therefore, in dealing with its contractors, DoD should be creating the best environment to ensure supplier security and resilience. Industry is the source of the new technologies to protect those technologies and can provide innovative means, operational and technical, to defend them. Industry often can respond more quickly and with more advanced, difficult-to-defeat technical measures than can government counterparts. Getting the best and most out of industry should be DoD's objective and is a primary element of *Deliver Uncompromised*. Adversaries know to attack those elements of the supply chain that have done the least. For this reason, DoD has to strike a balance—*incentivizing* best practices and company initiative on the one hand but *requiring* sufficient security measures on the other. The ultimate goal of the Department, to reduce *operational risk*, is promoted by measures that supplant *compliance* considerations as drivers and add *positive incentives* for companies to continuously examine and improve their systems and practices. This subject is addressed in *Annex III*.

Elsewhere in this report, we recommend a WOG approach to addressing supply chain resilience and integrated risk management. In some respects, this is only half the equation. As the character of warfare has changed, future battles may be fought, lost, or won within the industrial base. That base includes not only suppliers and integrators that specialize in defense acquisitions, but many other sources—some "commercial" and even "commercial off the shelf (COTS)"—whose products and services are incorporated in defense systems and infrastructure operation. For this reason, next-generation security merits a "whole of industry" approach. Beyond what can be accomplished with companies that are government contractors, leaders should consider how to establish and implement security and resilience standards to cover commercial sources and COTS suppliers. Otherwise, vulnerabilities at the weakest link remain. Because DoD is a major purchaser of supplies and services from the acquisition vehicles of other agencies, such as the General Services Administration Schedule 70 Governmentwide Acquisition Contract or the National Aeronautics and Space Administration Solutions for Enterprise-Wide Procurement, it will be necessary to extend the coverage of contract measures and validation methods to the contracting vehicles of civilian agencies for the acquisition of commercial IT products and product-based services. As demonstrated vividly by the experience with Kaspersky Labs software, attention must extend to commercial software as well as open-source software content that drives systems on which the government and the private sector rely.

10. Extend the 2015 National Defense Authorization Act (NDAA) Section 841 Authorities for "Never Contract with the Enemy" (MT).

The Combatant Commands, being forward-deployed outside the Continental United States, often in hostile and always in high CI threat environments, have unique supply chain and system integrity acquisition (contracting) and operational needs. They lack dedicated DIA/DSS interface, receive little in the way of warning, and when they do, there is no formal requirement for the Commander to act on such potential threats. Formation of the NSIC, as recommended above, would be extremely helpful to the Combatant Commands, as they would ultimately have a handful of liaisons with ready access to threat intelligence. In the meantime, adequate Joint Staff representation with DSS's expanded authorities as elsewhere recommended would support NSIC or interim entities.

To directly address these shortcomings, DPAP has drafted legislation that includes modifications of sections 841-843 of the NDAA, which goes back to 2012 and was modified in 2015. The draft legislation, which was approved by OSD, the Combatant Commands, Office of the General Counsel, and OMB, to shore up operational environment contracting overseas, includes proposed modifications for the 2019 NDAA. DoD should actively engage with Congress and the Executive Branch to build a strong support base to extend these authorities to the Combatant Commands. The recommendations that concern extension of these statutory authorities are summarized in *Annex IV.*

Contractors also have a role to play to avoid purchases from compromised and high-risk sources. Already, leading commercial companies go to great lengths to verify and monitor the trustworthiness of their supply chain. These should become prevailing if not expected practices within the defense supply chain. For certain types of key systems or technologies, it may be necessary to limit suppliers to U.S. sources or to validated international sources. Companies in the DIB should be encouraged to take measures to identify, mitigate, and then eliminate dependencies upon at-risk foreign sources.

11. Institute Innovative Protection of DoD System Design and Operational Information (MT).

Much of U.S. defense and intelligence has confused the concept of "need to know" with "classified." As a result, vast amounts of information regarding system design, trades, vendors, parts lists, operational details, etc., are usually available to *anyone* on the program, and much of it is available to the general public if they desire to go looking for it. Yet the commercial world treats its IP much more carefully and is much stricter concerning not only *who* they share their information with but *how*. Minimally persistent information sharing—much like that used in applications such as

Snapchat—in which minimum information is shared with a subcontractor or vendor via a thin-client network and only available for as long as needed—is becoming industry best practice in some circles. Some elements of the DIB are voluntarily using such techniques on defense contracts without being asked to by the USG. DoD could require such state-of-the-art techniques and compartmentalization based on need-to-know as a part of its basic information protection plan within the Department as well as contractually with suppliers.

Furthermore, where a program is in its life cycle is a determining function of what kind of protective measures are available (see Figure 2). Key capabilities that have been in operational use for decades are likely well known by our adversaries. As a result, their operational assurance risk should be considered high, and for the most vital ones, DoD should seriously consider increasing the ambiguity and uncertainty of the adversary with respect to these programs. Programs early in their life cycle are the easiest to protect, but that commitment needs to be made *at conception* and maintained through the life cycle.

There is a wide range of special options available for the most important programs, but each is different, depending on where the program is in its development cycle (from conception through retirement). The options exercised will become classified, but there will be tens of these, not hundreds.

12. Institute Industry-Standard IT Practices in all Software Developments (MT).

Software Bill of Materials (SBOM)

The software industry has progressed tremendously in the past several decades. Software is the "glue" that binds together components, systems, subsystems, sensors, etc. It is through software instructions that information moves to produce data-based decision making in complex instantiations of hardware. As software has acquired central significance in many systems of ever-expanding complexity, great change has occurred in how software code is created, compiled, and used. The software of complex systems is often built from many discrete software modules that perform distinct functions. Modern software can be rapidly or even automatically assembled. In this respect, software development increasingly resembles manufacturing processes. Thus, it is likely that any given custom or commercially available software system is, in fact, a product of a varied and often complex supply chain. Yet, all too often, and especially with open-source software, little is known concerning the pedigree of the software developer (who owns or controls the developer, for example) or the provenance of the software components (what measures were taken to ensure its integrity and trustworthiness).

In recognition of this fact, good industry practices increasingly mandate the use of an SBOM that identifies the provenance of the various components. If done properly, an SBOM can estimate the overall risk of the ensemble of software elements based on the risk of the individual elements. A dramatic increase in the security of operational software instantiations could be achieved by combining independent continuous monitoring of the development system and operations, independent integrity scoring of the contractor/vendor, and some type of real-time anomaly/event detection for the operational system.

Tracking software composition across the supply chain beyond the primary contractor/vendor is highly recommended and can be leveraged as a contractual term. Acquisition contract language should require the disclosure of commercial, open-source, and third-party software components as part of an SBOM. These disclosures should be independently verified. Knowingly providing false information should be subject to liability for damage and other sanctions against responsible contractors. DoD should not continue to do business with or use software sources that fail to deliver software uncompromised and those that submit false, misleading, or incomplete information. Taking such an approach as this is believed to be consistent with trends in the private sector and is recommended as a tenet of best industry practice.

Secure Software Design Life Cycle (SSDL)

The SSDL is a process DoD could apply to integrate security and integrity into the software development process from concept through decommissioning. This life-cycle approach to the software integrity challenge, blending security and risk identification and management across the acquisition and sustainment boundaries, will require true institutionalization of integrity and accountability in the chain of command. This process should begin with planning and requirements and continue through architecture and design, testing, coding, release, and maintenance. Simply "testing" or "certifying" once during Initial Operating Test and Evaluation is not only inadequate but signals to the adversary exactly when and how to "get past the gate" of security. By utilizing SBOM with continuous monitoring of the development environment coupled with SSDL techniques, this exposure can be reduced, resulting in a tangible realization of software integrity and a greater understanding of risk. The objective is for software security and integrity to become a *continuous* rather than a time-specific concern—from concept to retirement.

DoD can take a wide variety of SSDL approaches to software development that go well beyond the scope of this report. Industry best practices include use of code scanning tools both statically and dynamically and the establishment of realistic security goals and the means to measure progress toward them.

13. Require Vulnerability Monitoring, Coordinating, and Sharing across the Chain of Command for Supply Chain (MT).

While execution of a specific exploit against a particular program or capability may seem local, in reality, it is likely part of a more organized asymmetric offensive strategy against the United States' ability to project force or for the adversary to collect intelligence, steal IP, or otherwise gain a competitive advantage. Therefore, information sharing and the results of vulnerability monitoring are critical elements of an integrated defense. While the NSIC will provide strategic warning and insight into the risks of dealing with individual vendors/contractors or components, valuable information for the counterintelligence picture across the Department comes from the programs and operational Components in the form of self-reporting and observations of anomalous or suspicious activity or behavior. Currently, even within a Service Component, clear examples of incident reporting and potential exploitation are rare. While DSS enjoys a reliable stream of sharing from the DIB, its current purview is constrained to cleared facilities and the contractors using those facilities. Each Service Component in both acquisition and sustainment should look for and coordinate information sharing among themselves and with designated software vulnerability information sharing mechanisms such as the CVE® database, ISACs, the NTIA, the National Cyber Awareness System of US-CERT, and reports of the Computer Crime and Intellectual Property Section of the DOJ. Many of the COAs recommended by this report reinforce this discovery and sharing.

A vendor vetting database should be created and available to all. This could be championed out of DSS, DPAP, and NSIC. This database would house relevant acquisition, intelligence, and security information related to supply chain risk.

14. Advocate for Tax Incentives and Private Insurance Initiatives (LT).

There is a range of viable options for incentivizing members of the DIB to embrace cyber and supply chain security—especially the smaller subcontractors that are likely to be the most attractive targets of hostile actors. A central theme of this report is that DoD should examine ways to transform risk-management security functions from a cost center to a potential profit center—and a critical differentiator in the source selection process. We have identified and briefly described two categories that would produce positive financial incentives for the DIB—tax and insurance—and suggest other business initiatives to influence private sector actions. These measures would serve the congruent purposes of protecting contractor IP and protecting DoD technical data and other sensitive but unclassified information. DoD can make legislative proposals or otherwise advocate to Congress. This subject is addressed in *Annex V*.

15. For Resilience, Employ Failsafe Mechanisms to Backstop Mission Assurance (LT).

Beyond exploitation aimed at intelligence collection or harvesting of U.S. intellectual property, the objective of asymmetric adversary warfare is to degrade DoD's ability to execute its missions. The adversary has choices among targets. It may be able to achieve its ends largely, even entirely, through asymmetric operations launched against the private sector. An example is where an attack upon commercial logistics systems or transportation infrastructure denies the United States the ability to move forces when and where needed. Adversaries likewise target DoD capabilities directly. As shown in Figure 2, the ultimate exposure of such actions is where the consequence of attack, in the risk equation, produces a "fatal" result—denying readiness for mission. Means must therefore be identified to understand what critical systems are at risk of attack that could reduce them to a non-mission-ready state, and institute techniques that restore systems to a "fixable" state where mission execution continues even in a degraded state until full restoration is achieved.

The high-level, fundamental means of accomplishing resilience, from a system design perspective, is the use of "uncorrelated means of accomplishing the mission." In other words, there should be no single points of failure for critical mission elements—resiliency should be realized through smart system design, implementation, diversity, and redundancy. This can be done at the component, subsystem, system, and even enterprise level. For example, if command and control is singularly dependent upon satellite communications, then alternate means of enabling even degraded communications must be designed into the system to provide a failsafe mechanism. Ideally, different design teams, vendors, and contractors would design these failsafe backups, and collective knowledge of the entire system operation would be closely held. Realistic exercises should be conducted to inform mission owners of where they are at risk and how to recover.

A similar practice is utilized in the commercial world today, although often driven by the extremely high financial cost of loss of operational capability due to non-malicious events. For example, Amazon Web Services has multiple levels of failsafe mechanisms built into its architecture at the board, rack, building, micro geo-location, and macro geo-location—originally to ensure that when someone drops an item in their shopping cart, that information is not lost should a portion of the system fail.

This same type of integrated, integrity-based thinking needs to become pervasive within system engineering and design of DoD capabilities and could be a focus of OSD(R&E).

Conclusion

As a nation, we are at a watershed moment as the character and arguably even the nature of war is changing. There is now overwhelming evidence that adversaries employ blended operations in asymmetric warfare to steal our intellectual property, compromise our technical information, and to degrade, deny, or otherwise damage our factories and critical infrastructure. It is necessary to cast aside historical assumptions that have proven more to trap us than to protect. It is time to put legacy methods behind us. While we should be informed by the past, we should not become its prisoner. Therefore, the Department of Defense must lead initiatives to reduce exposure to hostile acts and enhance security of assets and capabilities. There are many initiatives to be combined and managed. Some affect the internal operations of the Department. Some are directed at the industrial base upon which DoD relies. And some require the coordination of resources among intelligence sources so that threat information can be rapidly processed to produce and appropriately distribute actionable strategic warning. The effort will take time and will present many challenges—but perpetuation of the status quo is unacceptable. We are past the time we can be satisfied with responses that are incidental or merely incremental.

The *Deliver Uncompromised* strategy merits leadership attention and immediate action. In the near term, *Deliver Uncompromised* means that mission owners can trust that the industrial base will not confer technical information or information advantage to adversaries. Means to achieve *Deliver Uncompromised* include elevating *security* as a primary metric for DoD acquisition, forming a Whole of Government National Supply Chain Intelligence Center, using existing acquisition authority and contracting leverage, and taking measures internal to the Department to empower leadership, better inform decision makers, and use accountability to spur results. This all needs to be done in concert with an incentivized and rewarded DIB.

DoD requires a Global Campaign Plan that goes well beyond countering terrorism—one that will defeat asymmetric threats being perpetrated against the United States. This report can serve as the foundation for a comprehensive strategy to defend the procurement and sustainment of the capabilities upon which DoD depends.

Annex I: Contractual Measures

Efforts are needed to create standards for security sufficiency that comprise a "standard of care" expected contractually of every company in the DoD supply chain. Medium and small-sized suppliers frequently complain that they need consistency and coordination in establishing security credentials to the satisfaction of DoD or higher tier contractors. We recommend that DoD and Industry establish a system and process to produce SIS, as introduced earlier in this report.

Industry is likely to have more trust in such a system if it is administered by an independent, expert, public-private body that would work with government, standards-setting bodies, industry, academia, technical specialists, and other interested parties. This entity would be able to receive classified materials so that the rating system would reflect the changing threat landscape. We envision the organization acting as an accrediting intermediary. DoD could establish levels or tiers of security sufficiency (Low, Moderate, and High, for example). The public-private entity could work with and for industry to guide, assess, accredit, and even authorize. Credentials received by a supplier through this process could be leveraged to demonstrate assurance to many potential defense customers and other public (or private) sector clients.

This report contains various contracting recommendations. Some will require new regulations and contract clauses. A few might require new statutory authority and rulemaking. To accomplish these will be time-consuming, and there may be uncertainty and questioning from some in the DIB. Those are not reasons to refrain from new action. The plain truth, however unfortunate, is that too many of the Department's present programs and operations already are compromised. Expecting better from our adversaries in the future, or believing that these problems will resolve themselves, would cause optimism to triumph over reality. However difficult, bold new action is required, and the acquisition process—broadly understood—is essential to positive change. Below, we summarize key concepts for using contractual leverage:

The "Plain Truth" Calls for Bold Action

The plain truth, however unfortunate, is that too many of the Department's present programs and operations already are compromised. Expecting better from our adversaries in the future, or believing that these problems will resolve themselves, would cause optimism to triumph over reality.

1. Achievement of minimum security measures can be required for companies (at any level) to participate in the defense supply chain for certain acquisitions.
2. Beyond trusting contractors to provide "adequate security" as required by DFARS 252.204-7012, the Department can establish measures and methods to review and assess actual accomplishment of promised security measures.
3. The Department can work with industry to establish metrics for enterprise-level accreditation of accomplished security using expert third parties for assessment. Use of SIS could motivate improved industry measures.
4. In determining eligibility for new awards, the Department can review the adequacy of required security measures, consider SIS, insist upon specified levels of accreditation, or otherwise

direct requiring activities to make authorization decisions based on their assessment of perceived risk for their specific missions.

5. Where competitive source selection methods are used, DoD can treat security as an evaluation factor and make superior security a positive competitive discriminator. RFPs would inform companies of what is expected and how it will be reviewed.
6. For software assurance, in appropriate contracts DoD can require source code disclosures, minimum maintenance and patching, continuous monitoring, and mandatory event reporting.
7. Using established safeguards, methods, and practices, DoD could establish minimum "standards of due care" such that gross negligence could expose contractors to civil liability or limit their eligibility for future contracts or subcontracts absent satisfactory corrective measures.
8. Contractual "safe harbor" provisions could be used to encourage positive security actions by contractors and to remove present barriers to prompt incident reporting and full cooperation with DoD's assessment and remediation measures.
9. Once appropriate standards are in place, DoD could require contractors to have specified levels of cyber and supply chain insurance.
10. DoD can improve its oversight of contractors to include review of cyber and supply chain assurance measures. DSS can extend its present responsibilities beyond cleared contractors.

Annex II: Litigation Reform Measures

Areas Where Litigation Exposure Should Be Reduced

It is advantageous for DoD that industry reports promptly and fully on known or suspected cyber and supply chain attacks and discovered software vulnerabilities. The DIB and its suppliers need to improve their record of reporting cyber incidents, supply chain vulnerabilities, and assurance failures. Potential litigation risk is part of the problem—both for industry and government.

- Contractors need "safe harbors" to promptly share suspicious or potentially derogatory information with NSIC for its assessment of and appropriate action on potential cyber and supply chain exploitations. Legislation or new regulation may be needed to establish that contractors making good-faith, informed reports on cyber and supply chain attacks will not be exposed to third-party lawsuits challenging the validity of such reports or seeking damages against the reporting entity. For this to occur, contractors need assurance that NSIC can protect the identity of reporting entities and keep reports confidential. NSIC will need to develop protocols on how to disseminate threat and response information based upon the reports.
- DSS has demonstrated the ability to leverage its existing contractual authorities for facility clearances; more robust information sharing on behalf of contractors would go much further with appropriate liability protections. Companies seeking to be treated as "trusted suppliers" can be asked to agree to higher obligations of event reporting and terms of participation in information sharing. New initiatives should be informed by present experience, such as that acquired by the Defense Microelectronics Activity in its trusted accreditation program. In this initiative, DoD must remain cognizant that suppliers will accept costs and burdens of specialized security regimes only if there is a corresponding business case that covers the costs and offers opportunity for profit.

- The government may need litigation reform to act upon industry reports or inputs from other public or non-public sources. Reporting is likely to have the highest value where it can be accomplished quickly. Speed is of the essence. Delays caused by legal review and process can work against the national interest. If the government acts to publish and disseminate contractor-sourced information, it may be exposed to third-party liability under the Federal Tort Claims Act (FTCA), 28 U.S.C. §§ 1346(b), 2671-2680, unless it can claim an exemption such as that for "discretionary function." The exigencies and gravity of cyber and supply chain threats may call for national security exceptions to standing laws and regulations. For example, a new FTCA exception could provide a basis for the federal government to claim immunity from third-party claims arising from cyber alerts and actions.

  DoD and WOG should have a set of tools to benefit its contractors and their suppliers who invest to develop new technologies for cyber and supply chain defense. These can run the gamut of functions—Identify, Protect, Detect, Respond, Recover—that the National Institute of Standards and Technology (NIST) has identified as the Core elements in the *NIST Framework for Improving Critical Infrastructure*.

- The *SAFETY Act*, administered by DHS, encourages investment in anti-terrorism technologies through liability limitations for qualifying, approved products, equipment, service, devices, and technologies. DoD should encourage Congress to extend this aspect of the SAFETY Act to cyber and supply chain security investments. Companies that make such investments and utilize new security systems should face reduced exposure to third-party and government claims following a cyber or supply chain attack. The immunity should extend also to subcontractors and suppliers who employ validated technologies.

- Industry needs to have confidence in the efficacy and expertise of the persons or entities assigned the responsibility to assess and qualify the cyber and supply chain technologies eligible for SAFETY Act liability protection. Consideration is warranted of assigning this function to a trusted third-party intermediary (public or private) that can concentrate expertise, promote new standards and best practices, secure valuable contractor IP, and coordinate with DoD and other government resources for their input and, if appropriate, approval. Potentially, the same independent intermediary that conducts assessments and assigns SIS could perform the SAFETY Act reviews.

Areas Where Liability Risk Might Be Increased

With limited exceptions, it is at best uncertain where or under what circumstances any DoD contractor would face liability to DoD for damages should it fail to fulfill minimum contractual requirements for supply chain and cyber security. Under present law, action could be brought under the False Claims Act for knowing or reckless disregard of cyber obligations, or for intentionally false promises to operate with security that were not fulfilled. To be sure, no contractor or commercial enterprise can guarantee that it will not suffer cyber or supply chain attack, and the fact of attack should never be treated as evidence, itself, of fault on the part of the entity attacked.

Nonetheless, if there is little or no prospect of monetary liability to the DoD customer, and where there may be no financial consequences for bad cyber and supply chain hygiene, some companies may ignore their promises, and others will fail to commit sufficient resources and attention to security improvement. DoD should examine where and on what basis, and with what process, it could expose contractors to contractual damage liability for failure to take reasonable and timely cyber and supply chain assurance measures. Even if the bar is set very high for a contractor to be held liable for breach of expected minimums for assurance, the prospect of such litigation and potential liability may have salutary effects upon

management commitment and company actions. Moreover, the Department may consider whether to seek legislative authority and a regulatory basis to hold its contractors, on selective programs, liable for gross negligence in failure to fulfill cyber and supply chain commitments.

Software liability is an area that merits close attention. Vulnerabilities arise from poor software security, yet it remains the prevailing commercial practice not to make users and operators responsible for software-caused failures and to immunize those who developed the software. For its mission-critical and specially developed software, DoD can demand higher security across the software development life cycle, especially in projects that involve agile or DevOps environments or software refresh during sustainment. Much of the software used in contemporary systems has open-source components with uncertain pedigree or provenance. DoD should consider when to require an SBOM and can encourage Congress to hold hearings on whether to change the law on software immunity—perhaps for certain areas of commerce related to national security and industry and key infrastructure.

It remains true that a hostile actor instigates software, cyber, and supply chain attacks, and therefore, the initiating responsibility resides with the attacker. Today's security environment, however, is one in which such attacks are a fact of life. The attacks are recurring, persistent, diverse, evolving, and highly destructive. In this environment, those who own and operate systems at risk of these threats have a duty of due care to take actions *reasonable*, in light of what they know of threat, vulnerability, and consequence, and *responsible*, considering their resources and technical capabilities. Some analysts have argued that the prospect of civil litigation in the courts and liability for damages will prove important to move the whole of industry to act. The standard of care will figure prominently in what companies do to mitigate litigation risk. DoD has a responsibility to establish and incentivize cyber and supply chain standards that will set a standard of care that is achievable and affordable for the DIB and its suppliers.

Annex III: Ensure Supplier Readiness and Use Contract Terms

The Department should communicate to all levels of the supply chain that integrity is both expected and rewarded, for continuing DoD business, and that *delivering* uncompromised and resilient products is an integral part of contract performance—equal (at least) to cost, schedule, and performance.

Supplier Readiness

DoD can exercise creative options to ensure supplier readiness.

- DoD can work with industry stakeholders to establish cyber and supply chain security standards and practices, and software assurance measures, building off the increasing volume of NIST work that integrates cyber and supply chain measures.

NIST has issued a proposed Revision 5 to SP 800-53 and the Cybersecurity Framework v. 1.1, which encourage important progress in elaboration of combined cyber and supply chain measures. Indeed, the just released SP 800-37 Revision 2 includes the following concise statement of purpose:

"To integrate supply chain risk management (SCRM) concepts into the RMF [Risk Management Framework] to protect against untrustworthy suppliers, insertion of counterfeits, tampering, unauthorized production, theft, insertion of malicious code, and poor manufacturing and development practices throughout the SDLC [System

Development Life Cycle]."
Draft SP 800-37 Rev. 2, at vi.

- As companies act to implement these safeguards, they can be evaluated and assigned into tiers of relative security. Previously in this report, we introduced the idea of SIS. A similar approach is used elsewhere in the federal government. For example, the NIST Cybersecurity Framework articulates four Implementation Tiers in a range from Partial (Tier 1) to Adaptive (Tier 4). Federal Information Processing Standard (FIPS) 199 distinguishes among security impact at levels of Low, Moderate, and High. As elaborated in FIPS 200 and NIST SP 800-53, obligations for controls and enhancements are linked to the impact level of information at risk. The implementation of the Federal Risk and Authorization Management Program (FedRAMP) is particularly instructive. FedRAMP provides a standardized approach to security for cloud computing and for the authorization of cloud services for civilian agencies. In simplified form, FedRAMP produces Authorization to Operate for federal customers for Low-, Moderate-, and High-impact systems. DoD has special requirements for cloud, but again it is a hierarchy of information sensitivity, with more security required for higher Impact Levels. The Defense Information Systems Agency has produced the *Security Requirements Guide*, which adds overlay of both process and substantive security requirements building on FedRAMP, again relying on NIST SP 800-53 as the catalog of available controls.
- For cyber and supply chain assurance, we envision that DoD can work with industry to specify which assurance methods and measures must be met for a contractor to earn a Low, Moderate, or High SIS. Each requiring activity (or each prime contractor) can decide whether its program requires the additional measures (and expense) of a supplier with a higher score, and what evaluation credit to extend for competitors with different score levels. For FedRAMP, the security assessment process is the responsibility of independent third-party assessment organizations working to government-approved process and standards. For the SIS process, we see merit in following a similar approach that allocates the assessment and scoring responsibility to accredited third parties.
- Both suppliers and DoD will benefit if security credentials, established once, can be leveraged across all DoD Requiring Activities. The same approach—"do once, use many times"—can be applied to assessment of suppliers and SIS. Documentation that supports the assigned rating can be available for review by requiring activities within the Department. This prevents duplication of assessment. DoD can require that companies awarded an SIS credential conduct continuous monitoring, and the status as a holder of a credential can be subject to review and renewal at specified intervals. This too is like FedRAMP. It also is similar to the process DSS uses in the grant of Facility Clearance Levels.

It may take some time to establish this credentialing regime, to establish expected methods and assessment process, and to resolve questions of roles and missions among many potentially interested stakeholders. There can be high payoff, however.

Acquisition and Contract Terms

DoD has great influence, through the acquisition process, on the companies that constitute the DIB supply chain. The Department can make better use of these tools to achieve and sustain cyber and supply chain security.

- DoD, through DFARS 252.204-7012, requires all its contractors to have "adequate security" to protect Controlled Unclassified Information (CUI), relying on the 110 safeguards in NIST SP 800-171. Today, there is no method or requirement for assessment, as the implementation is largely trust-based. Moreover, DoD has not assigned a qualified resource to review the actual security accomplishments of

its suppliers. Further, the SP 800-171 safeguards treat all information as having essentially the same, Moderate impact should a breach occur. In addition, DFARS and SP 800-171 focus on the protection of information on or in information systems—with little coverage of supply chain security or operations technology as distinct from IT.

- In the dynamic threat environment, the Department needs to pursue a strategy and campaign to elevate the level and expand the breadth of security achieved, and to implement means of review, assessment, approval or authorization, and oversight. These must be pursued gradually because the present requirements, notwithstanding their limitations, have proven to be very difficult for a sizable percentage of the DIB. DoD must retain the innovation and versatility of the smaller members of the industrial base, and it must work with its prime contractors to assist companies struggling with security requirements. Specifically, DoD should encourage primes and their small business suppliers to shift information systems and applications to qualified, secure cloud service providers. The security outcome for many companies using the cloud will be superior compared to measures taken for on-premises systems. Updates, information management, and cybersecurity are all improved with a cloud provider, since responses can be done on scale and quickly, by not relying on individual patching. DoD is moving aggressively to the cloud, and requiring the DIB and its sub-tired suppliers to follow suit is a logical and practical solution.
- The Department has its greatest leverage, of course, over prime contractors. As evident from Enclosure 14 of Department of Defense Instruction (DoDI) 5000.02, DoD already includes cyber as an objective in the acquisition planning for MDAPs. Similar improvements could be made to DoDI 5000.02, and to the accompanying Defense Acquisition Guidance, to give greater importance to supply chain and software assurance.
- Incorporation of further objectives in acquisition planning should translate to additional definition of cyber, supply chain, and software assurance in program requirements as expressed in Statements of Work and specifications. Funding should accompany these changes, as security has a cost.
- DoD is already acting to inform contractors that they may be required to submit System Security Plans (SSPs) for evaluation and adequacy determination in the source selection process. DoD recently proposed guidance for Contracting Officers on when to request SSPs and how to evaluate their adequacy. Further measures along these lines should be established as security standards and assessment processes develop. DSS, in line with its new emphasis on asset protection, should be considered for increased responsibilities to assess and validate contractor measures to secure CUI.
- Prime contractors undoubtedly will strive to improve and demonstrate their security accomplishments where a source selection includes comparative evaluation and scoring of each offeror's security. At the same time, contractors will insist upon a fair process in which they understand in advance what is expected of them and how it will be evaluated. Having the process defined and resources in place will take some time. But contractors should be informed now that DoD is working to make security a competitive discriminator in future procurements.
- Beyond the prime, as noted, security risks are present at the lower tiers, where DoD has less leverage and no direct contract authority. Clearly, the Department needs to reinforce cyber and supply chain security at every level. Such initiatives will have significant effect upon thousands of private sector enterprises. Some of the responsibility will vest in the primes and higher tier companies. As suggested above, establishing a mechanism for credentialing using common standards and a consistent process will be most helpful. It will

reduce friction within the private sector and avoid unproductive expense and frustration of attempting to conform to multiple, inconsistent reviews and demands.

It may be necessary to reconcile procurement reform with security enhancement. There is widespread enthusiasm for measures to "reform" procurement to reduce barriers to commercial sources, encourage innovation, speed purchase and delivery, and eliminate unproductive regulatory costs. The Department should consider the tension between security objectives and procurement reform. Security measures, as recommended here, should not be just "more cost and time" but should add to the bottom line and be integrated into the procurement process. In acquisition planning, DoD may need to distinguish, and treat separately, acquisitions for high-impact platforms and programs and involving sensitive but unclassified technologies. It will not always be possible both to reform procurement to make it faster, cheaper, and more accessible to commercial suppliers, and to improve and sustain the security of the suppliers. Choices and priorities need to be established and shared with the DIB.

Annex IV: Proposed Section 841-843 NDAA Authority Extensions—Never Contract With the Enemy

	NDAA 2012 Subtitle D – Provisions relating to Contracts in support of Contingency Operations in Iraq & Afghanistan	NDAA 2015 Subtitle E – Never Contract with the Enemy	NDAA 2019 (If enacted into bill) Subtitle X – Never Contract with the Enemy
Applicability	DoD; Contracts greater than $100K performed outside U.S. in CENTCOM AOR	WOG; Contracts performed outside the U.S, greater than $50K, in support of a contingency operation in which members of the Armed Forces are actively engaged in hostilities.	WOG; Contracts performed outside the U.S. (or inside the U.S. to foreign vendor(s)) regardless of dollar value and operation type
Identification Authority	SecDef through CENTCOM Commander—"identified by the Commander of the United States Central Command"	"the SecDef shall…establish a program…" (24 Jan 17—OSD formal Legal opinion confirmed SecDef ID authority until delegated)	SecDef until delegated down through implementation policy
Identification Criterion	…provides funding directly or indirectly to a person or entity that has been identified by the Commander of the USCENTCOM as actively supporting an insurgency or otherwise actively opposing U.S. or coalition forces in a contingency operation in the USCENTCOM theater of operations. …failed to exercise due diligence to prevent funds from being provided to a person or entity actively opposing U.S. or coalition forces…	(1) provide funds, including goods and services,…directly or indirectly to the enemy (2) fail to exercise due diligence to ensure that none of the funds, including goods and services,… are provided directly or indirectly to the enemy	1) provide funds, including goods and services,…directly or indirectly to a covered person or entity; (2) fail to exercise due diligence to ensure that none of the funds, including goods,… are provided directly or indirectly to a covered person or entity; (3) directly or indirectly support a covered person or entity or otherwise pose a force protection risk to United States Government agencies or Coalition Forces; or (4) pose an unacceptable national security risk.
Covered Person or Entity aka "the Enemy"	Person or entity actively supporting an insurgency or otherwise actively opposing United States or coalition forces in a contingency operation in the United States Central Command theater of operations	A person or entity that is actively opposing United States or coalition forces involved in a contingency operation in which members of the Armed Forces are actively engaged in hostilities.	A person or entity that is (A) engaging in acts of violence against the U.S. Gov't agencies or coalition forces, or providing support, in the form of financing, logistics, training, or intelligence, to those that do; (B) directly or indirectly opposing the interests of U.S. Gov't agencies or coalition forces; (C) engaging in foreign intelligence activities against U.S. Gov't agencies or coalition forces; (D) engaging in transnational organized crime or criminal activities. E) engaging in other activities that present a direct or indirect risk to the national security of the United States or coalition forces;

Annex V: Tax Incentives and Private Insurance Initiatives

Supply Chain Tax Proposals

Tax incentives are a powerful and effective tool to shape corporate behavior in the supply chain process. Tax credits, subsidies, new market incentives, and capital gains rewards are some of the potential ways to make supply chain security investment and deployments profitable. Some proposed recommendations to be explored:

- Tax Credit/Subsidy for Supply Chain Security
  Tax credits or subsidies, such as 26 USC § 48C, or the energy credit in the tax code, have encouraged the use of solar power, wind turbines, fuel cells, and heat pumps. The business energy investment tax credit was passed as part of the Energy Policy Act of 2005 and allows for a 30 percent offset of an investment in an alternative energy system. Similarly, companies that deployed state-of-the-art security would apply for specific tax credits for the taxable year the innovations or products were deployed and could enjoy a similar type of discount. Moreover, tax credits could be used to improve security at lower levels of the supply chain. Apart from encouraging investments by individual vendors and suppliers, a tax credit or rebate could be offered to primes that make investments that improve the means available to subcontractors to improve security, such as offering security as a service.
- New Market Tax Credit Model—Small Businesses
  The new market tax credit program 26 USC § 45D, established as part of the Community Renewals Tax Relief Act of 2000, helped usher in a wave of investment in low-income communities. The credits spurred investments by community development entities and were administered by the Treasury Department. The program was extended by the Tax Relief Unemployment Insurance Reauthorization and Job Creation Act of 2010, and was again reauthorized until 2014. This successful program could be adapted for supply chain purposes. Treasury could extend conditional subsidies as refundable tax credits for security investments by small businesses. If administered by Treasury, thresholds could be established and penalties imposed if fraud or gross negligence were found in a security breach.
- Capital Gains Tax Incentive
  This tax incentive would reward shareholders with a lower capital gains tax on the sale of assets of corporations that had voluntarily adopted certified and well-recognized supply chain security processes, frameworks, and applications. Investors and shareholders would have an economic incentive to pressure boards of directors to adopt state-of-the-art security measures. The approach would produce long-term value creation for shareholders and the corporations. The Securities and Exchange Commission could be a logical enforcement agency that would impose penalties for misrepresentation and help set security metrics.

Supply Chain Insurance Proposals

It has been estimated that the cyber insurance premium market has the potential to reach $7.5 billion in a few years. Currently the market is estimated to be in the $2.5 billion range. At this time there is no standardized federal policy that regulates cyber insurance carriers or coverage. Nothing now requires DIB companies to acquire insurance for cyber or IT processes. Private insurance carriers can play an important role in setting standards for coverage and in the assessment of enterprise security that figures into underwriting decisions. However, insurance coverage today is oriented toward liability protection against the financial consequences of a breach that produces loss of confidentiality of personally identifiable information or other commercial or consumer records subject to privacy requirements. DoD's interests are different. DoD may consider working with the insurance industry and the DIB to establish

coverage objectives, security norms, and use of DFARS contracting tools to require coverage.

It has been noted that the cybersecurity insurance market has remained tentative due to a number of factors—there is a lack of sufficient actuarial data; insurance portfolios do not have standardized categories of risk; and defense contractors lack the information to understand the scope of appropriate coverage. In contrast, the use of risk assessment is well established within the federal government. The recently released *Federal Cybersecurity Risk Determination Report and Action Plan* (May 2018) required by Executive Order 13800 emphasizes risk assessment, as does OMB Memorandum M-17-25 (May 2017). These subjects also are well explored by FIPS-199 and receive new emphasis in the recently released draft of NIST SP 800-37 Rev. 2, which is to "develop the next generation Risk Management Framework (RMF)." These provide a sound foundation for extension of risk assessment methods to the DIB and other private sector enterprises, and will help in establishing a set of agreed-upon metrics and taxonomy for cybersecurity, as they will facilitate increasing and effective use of insurance to improve supply chain security. We propose the following for examination:

- Support Creation of the Cyber Incident Data and Analysis Repository (CIDAR) at DHS or DoD
  The lack of actuarial data has been a major impediment to establishing a robust cyber insurance market and standardized policies. DHS has been exploring the possibility of creating a trusted space so member corporations could share anonymous sensitive cyber incident data, the CIDAR. This data collection and repository would provide this information to appropriate insurers so that standardized policies could be created. The process would help establish standardized categories and a common taxonomy for cyber incidents for the industry. This self-reporting should be conducted under the auspices of the Cybersecurity Information Sharing Act of 2015 (CISA) and its protection from liability (CISA § 106 (b)). The same concept could be undertaken by DoD, independent of DHS, building upon the existing DIB Cybersecurity Program and expanding information sources beyond present members who are cleared contractors and whose participation is voluntary.
- Government as Guarantor—Terrorism Risk Insurance Act (TRIA)
  Government should establish an insurance fund to cover the possibility of a catastrophic supply chain disaster of either a national cross-sector cascading effect of a cyber attack or an attack by a foreign power as an APT. TRIA was passed after 9/11 to provide compensation for large losses resulting from acts of terrorism so insurers would be able to recoup their losses as a national security asset. TRIA ensured the affordability of insurance for terrorism risk, built insurance capacity, and shared the losses between the public and private insurance sectors. In addition, a number of policies in the cyber insurance arena have "acts of war" or "act of God" exclusions, and in the event of a cyber intrusion by a foreign power, both the insured and insurers should have state protection.
- Amend DFARS to Require Insurance Coverage
  A standard contract clause could be added to DFARS requiring contractors to obtain commercial insurance coverage for cyber and supply chain security. The cost of such coverage would be an allowable cost. The Department could work with insurance carriers and industry stakeholders to develop the coverage objectives, metrics, and standards, as well as the methods to be used by carriers to assess and validate the eligibility of contractors for coverage. Accordingly, at the front end, the coverage process would utilize private sector resources (carriers and their third-party assessors) to promote adoption of security measures consistent with DoD's objectives. At the back end, the liability coverage would give assurance to companies that they are protected against direct damages and third-party liability in the event of any breach producing injury to enterprise

operations or compromise of DoD or other source data. This approach also would help establish a baseline of standards and practices and spread cyber and supply chain risk across the marketplace. Just as fire insurance places a number of structural requirements in building codes, based on the requirements of the cyber and supply chain insurance policy, the DIB would have to maintain fundamental standards in a variety of areas, such as (for illustration) encryption of data at rest. New security issues, such as those arising from the increasing use of IoT instrumentalities to connect enterprise systems, also are candidate areas to align DoD objectives with the private insurance industry.

- Use Authority of Public Law 85-804—Indemnification
  This rarely used authority, originally passed during World War II, provides contract relief and indemnification for companies engaged in unusually dangerous activity on behalf of the government. This power could be used to protect private companies against the possibility of extraordinary liability as might arise in working with DoD in high-risk cyber activities, including "full spectrum" measures. Public Law 85-804 also might be applied as a backstop of indemnification to encourage the DIB to share critical information on cyber breaches, should the existing CISA mechanism prove inadequate.

Other Supply Chain Measures

- IP Trusts and "Golden Shares"
  DoD remains reliant upon global sources, but some technologies and some sources are more critical than others. Measures may be needed to protect against the loss of specific sources or technology. The Department could enter into agreements with some DIB participants to create IP Trusts between prime contractors and key suppliers. The primes would be trustees, with the DoD as the third-party beneficiary. The trusts would protect the critical IP and companies entering the trust. In certain specified events, such as a change of control presenting concerns of foreign ownership, control, or influence, or where there is a disabling security breach at the subcontractor level, DoD could exercise its authority as trustee to recover IP in an uncompromised state. In the area of software assurance, a trust mechanism might be used to assure DoD that it has the gold standard of code for purposes of forensics, patch management, or other security or restorative measures. DoD could also be granted "golden shares" in the trust that would allow it to outvote all board members. In the event of a critical bankruptcy or potential sale, the authority over the golden shares would allow DoD to shape the outcome, enabling it to condition approval upon adequate mitigation measures or, if necessary, block ownership or technology transfers altogether, where potential transactions are found to violate national security interests.

Biographies

Christopher Nissen
Director, Asymmetric Threat Response
Special Concepts Group
The MITRE Corporation

Christopher Nissen is Director of Asymmetric Threat Response at The MITRE Corporation, a not-for-profit which operates and manages seven FFRDCs serving in the national interest. He works across the corporation developing essential strategic elements to address non-kinetic, full-spectrum asymmetric threats to national security in both the public and private sectors. He has developed extensive work programs in these and other domains across the technology, policy, and legislative solution spaces. He has also served as Director of the Communications and Networking Technical Center, leading a division of over 230 engineers in a diverse portfolio of programs and technology development spanning microelectronics to satellite communications.

He has 30 years of experience in developing solutions for extremely complex national security challenges. Some of his accomplishments include putting forth an original vision for the development of an anti-jam capability for the nation's Global Positioning Satellite system, and the development and implementation of several special communications techniques. He holds BSEE and MSEE degrees and also has a background in structured analytical techniques.

Deliver Uncompromised

John E. Gronager, Ph.D.
Director, Special Enterprise Capabilities

Dr. Gronager recently joined The MITRE Corporation as the Director of Special Enterprise Capabilities within the MITRE National Security Sector. He serves as a senior technical contributor in MITRE's cyber, critical infrastructure, nuclear, and supply chain work programs. In collaboration with MITRE's work program leaders, Dr. Gronager has worked to develop MITRE's work program, create intellectual capital, and identify and develop talent in these critical areas.

Before joining MITRE, Dr. Gronager had 38 years' experience in managing technical programs across the national security mission of Sandia National Laboratories. As a former Distinguished Member of the Technical Staff and Senior Manager, Dr. Gronager developed and managed programs in nuclear reactor safety, nuclear weapons design, testing, and manufacturing, the national transportation infrastructure, international security programs, and for over 28 years provided support to the Intelligence Community.

Robert S. Metzger, J.D.
Shareholder, ROGERS JOSEPH O'DONNELL, a Professional Law Corporation

Robert S. Metzger, an attorney in private practice, heads the Washington, DC, office of Rogers Joseph O'Donnell, P.C., a firm that has specialized in public contract matters for more than 35 years. He has an active practice that includes civil and administrative litigation, compliance counseling, national security matters, export issues, and other regulatory advice. Mr. Metzger represents leading U.S. and international technology companies in several industry sectors.

Mr. Metzger is recognized for subject area leadership in cyber, supply chain, and related security subjects and has many publications on these subjects. Named a 2016 "Federal 100" awardee, he was cited by *Federal Computer Week* for his "ability to integrate policy, regulation and technology." *Federal Computer Week* said of him, "In 2015, he was at the forefront of the convergence of the supply chain and cybersecurity, and his work continues to influence the strategies of federal entities and companies alike."

Chambers USA (2018) ranks him among top government contracts lawyers and said that "[h]e is particularly noted for his expertise in cyber and supply-chain security with clients regarding him as the 'preeminent expert in cybersecurity regulations and how they affect government contractors.'"

For RSA Conference 2018, Mr. Metzger served on a panel on "First Recourse or Last Resort? The National Interest in Regulating the IoT" and moderated a second panel on "IOT and Critical Infrastructures: A Collision of Fundamentals?" For RSA Conference 2017, he moderated a discussion on "Cyber/physical Security and the IoT: National Security Considerations." A member of the International Institute for Strategic Studies, his articles on national security topics have appeared in *International Security* and the *Journal of Strategic Studies*, among other publications.

The Legal 500 in 2016 cites Mr. Metzger as an "expert" in cyber and supply chain security; in prior years, he was recognized by *The Legal 500* for telecommunications (litigation and appellate). He is among the 49 U.S. lawyers rated as "Expert" in government contracts by *Who's Who Legal* (2016, 2017). He was featured in the Government Contracts 2017 Discussion of *Who's Who Legal*.

Mr. Metzger attended Georgetown University Law Center, where he was an Editor of the *Georgetown Law Journal*. Subsequently, he was a Research Fellow, Center for Science & International Affairs, Harvard Kennedy School (now, "Belfer Center"). As a Special Government Employee of the Department of Defense, he was a member of the Defense Science Board task force that produced the Cyber Supply Chain Report in April 2017.

Mr Metzger served as a subject-matter expert subcontractor to The MITRE Corporation for this study.

Harvey Rishikof, J.D.

Harvey Rishikof's career includes experiences in the private sector, academia, and public service. He is a lifetime member of the Council on Foreign Relations and the American Law Institute. Mr. Rishikof is currently Senior Advisor to the American Bar Association (ABA) Cybersecurity Legal Task Force, Chair of the Advisory Committee to the ABA Standing Committee on Law and National Security, and is working on a number of projects with MITRE and the MacArthur Foundation. For the next year he will be a Visiting Professor at Temple Law School. Mr. Rishikof was a Teaching Professor and Director of the Cybersecurity and the Law program in the iSchool and Earle Mack School of Law at Drexel University. He is the former Convening Authority for the Military Commissions and senior policy advisor to the director of the National Counterintelligence Executive in the Office of the Director of National Intelligence. He has held several positions in the National War College (NWC) at the National Defense University in Washington, DC, including Dean of the NWC, Chair of the Department of National Security Strategy, and Professor of Law and National Security Studies. Academically and professionally, Mr. Rishikof specializes in the areas of national security, civil and military courts, terrorism, international law, civil liberties, and the U.S. Constitution.

He is a former member of the law firm Hale and Dorr, the former Dean of the Roger Williams University School of Law, in Bristol, RI, and has been a consultant to the World Bank and the USAID on law reform. As Legal Counsel to the Deputy Director of the FBI, he focused on FBI policies concerning national security and terrorism, and served as liaison to the Office of the Attorney General at the Department of Justice. He worked on developing a variety of programs (e.g., the National Integrated Ballistic Information Network), and was involved in the drafting of Presidential Decision Directives in the national security area.

As Administrative Assistant to the Chief Justice of the Supreme Court (1994-96), Mr. Rishikof, a former federal court of appeals law clerk in the Third Circuit for the Honorable Leonard I. Garth, served as chief of staff for the Chief Justice and was involved in general policy issues concerning the federal court system. In this capacity, he acted as liaison to the Executive Branch, Congress, the Federal Judicial Center, and the Administrative Office of the United States Court.

Mr. Rishikof has participated in numerous international seminars and projects in Latin America, Europe, Russia, Southeast Asia, Pakistan, India, and China. His most recent books are co-edited with Roger George, *The National Security Enterprise–Navigating the Labyrinth* (Georgetown Press, 2d ed. Quad 2017) and co-edited with Stewart Baker and Bernard Horowitz, *Patriots Debate–Contemporary Issues in National Security Law* (ABA Press, 2012). Mr. Rishikof has participated in numerous international seminars and projects in Latin America, Europe, Russia, SE Asia, Pakistan, India, and China. His publications include *Morality, Ethics, and Law in the War on Terrorism (The Long War)*, part of

the West Point terrorism series Countering Terrorism and Insurgency in the 21st Century: International Perspectives.

Mr. Rishikof holds a JD from New York University School of Law, an MA from Brandeis University, an MA from the National War College, and a BA from McGill University.

Mr. Rishikof served as a subject-matter expert subcontractor to The MITRE Corporation for this study.

Acronyms

A&S	Acquisition and Sustainment
ABA	American Bar Association
APT	Advanced Persistent Threat
CI	Counterintelligence
CIDAR	Cyber Incident Data and Analysis Repository
CISA	Cybersecurity Information Sharing Act of 2015
COA	Course of Action
COTS	Commercial off the Shelf
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
DEPSEC-DEF	Deputy Secretary of Defense
DHS	Department of Homeland Security
DIA	Defense Information Agency
DIB	Defense Industrial Base
DNI	Director of National Intelligence
DoD	Department of Defense
DODI	Department of Defense Instruction
DOJ	Department of Justice
DPAP	Defense Procurement and Acquisition Policy
DSS	Defense Security Service
DU	Deliver Uncompromised
FBI	Federal Bureau of Investigation
FedRAMP	Federal Risk and Authorization Management Program
FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
FPAP	Field-Programmable Gate Array
FTCA	Federal Tort Claims Act
IC	Intelligence Community
IoT	Internet of Things
IP	Intellectual Property

ISAO	Information Sharing and Analysis Organization
IT	Information Technology
LT	Long Term
MDAP	Major Defense Acquisition Program
MT	Medium Term
NCSC	National Counterintelligence and Security Center
NCSC	National Counterintelligence Security Center
NCTC	National Counterterrorism Center
NDAA	National Defense Authorization Act
NIST	National Institute of Standards and Technology
NSIC	National Supply Chain Intelligence Center
NTIA	National Telecommunications and Information Administration
NWS	National War College
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
OTA	Other Transaction Agreement
OUSD(I)	Office of the Under Secretary of Defense for Intelligence
R&E	Research and Engineering
RFP	Request for Proposal
SBOM	Software Bill of Materials
SCRM-TAC	Supply Chain Risk Management – Threat Analysis Cell
SIS	Security Integrity Score
SSDL	Software Design Life Cycle
SSP	System Security Plan
ST	Short Term
TRIA	Terrorism Risk Insurance Act
TSN	Trusted Systems and Networks
TTPs	Tactics, Techniques, and Procedures
US-CERT	United States Computer Emergency Readiness Team
USD(I)	Under Secretary of Defense for Intelligence
USG	U.S. Government
WOG	Whole-of-Government

Deliver Uncompromised

MITRE

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),

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

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.

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

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-

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

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).

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

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/.

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

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).

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

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.

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

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.

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

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,*

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

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.

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

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*.

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

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.

IceMiller
LEGAL COUNSEL

July 7, 2020
Louis T. DeLucia, Alyson M. Fiedler, Jason M. Torf

Professionals
- Louis DeLucia
- Alyson Fiedler
- Jason Torf

Related
- Bankruptcy and Restructuring
- Creditors' Rights and Commercial Law
- Distressed Investments

Guidance for Purchasing Distressed Assets

The COVID-19 pandemic has caused economic turmoil that may provide opportunities for financially secure companies with capital to make a strategic acquisition of distressed assets and for investors to acquire valuable assets. The following highlights some important considerations when evaluating a purchase of distressed assets.[1]

How to Finance the Purchase of Distressed Assets

Often, distressed assets do not meet the criteria for traditional debt financing. There are a number of alternative ways to finance the purchase of distressed assets, including: (i) utilizing cash flow from purchaser's existing business; (ii) obtaining a secured loan from a lender with a security interest in purchaser's assets; (iii) using an asset-based lender ("ABL") to receive quick access to capital; (iv) seeking a loan from the seller's existing lender; and (v) potentially leveraging the acquisition by securing the acquisition financing with the target company's assets (an "LBO"). However, as discussed below, LBOs can be associated with increased risk of attack (a fraudulent conveyance action) by the target company's creditors, if the company is insolvent or rendered insolvent as a result of the LBO.

How to Acquire Distressed Assets

Buyers can decide whether to purchase distressed assets in a formal bankruptcy process, a state court insolvency (such as "assignment for the benefit of creditors" or "ABC") or receivership proceeding or to proceed out of court with a more traditional acquisition process.

Chapter 11 Bankruptcy and a 363 Sale

A chapter 11 bankruptcy traditionally involves a debtor proposing a plan of reorganization for the restructuring of its debts with the objective of continuing to operate. More often, however, chapter 11 is being used as a vehicle for distressed companies to sell some or all of their assets—commonly known as a "363 sales" in reference to the applicable section of the Bankruptcy Code. Following bankruptcy court approval of the debtor's "bid procedures," and after conducting an auction and selecting the highest and best bid, the debtor submits the proposed transaction to the bankruptcy court for approval. Approval of a 363 sale does not involve the same extensive voting and confirmation process required for approval of a chapter 11 plan. One of the greatest benefits to a buyer who acquires assets through a 363

sale is the conveyance of the assets by court order that conveys title “free and clear”—that is, the buyer takes the assets “free and clear” of all liens, claims, interests, and encumbrances against those assets, leaving those infirmities with the bankruptcy estate. The “free and clear” concept is memorialized in an order entered by the bankruptcy court approving the sale transaction. The holders of the liens and claims seek recovery on their claims from the proceeds of sale held by the bankruptcy estate while the buyer receives significant protection against acquiring unwanted liabilities including, often, successor liability claims. Further, a 363 sale eliminates the risk that the sale could be set aside as a fraudulent transfer that otherwise exists in out-of-court distressed acquisitions. In out-of-court transactions, valuation is important because creditors can challenge a transaction that was not for "fair and adequate consideration." The sale order entered in a chapter 11 process protects the buyer from such a challenge.

A buyer who identifies distressed asset acquisition opportunities early can further benefit by acting as the “stalking horse” bidder in a 363 sale. The stalking horse bidder is the baseline bid—both in terms of dollar amount and the various terms and conditions in the proposed asset purchase agreement—for an auction. A stalking horse bidder typically receives certain bid protections, such as a break-up fee (i.e., a fee payable to the stalking horse bidder if another bidder ultimately is selected as the winning bidder) and an expense reimbursement to compensate the stalking horse bidder for its time and investment in the process (which can be argued to set a benchmark for bidding that brings value to the bankruptcy estate). Not only do these bid protections offer compensation in the event that another bidder is selected as the winner after an auction, but they also offer an advantage to the stalking horse bidder during an auction because other bidders will need to outbid the stalking horse bidder by at least the value of the bid protections to make the alternative bid more valuable to the bankruptcy estate than the stalking horse bid. Conversely, the stalking horse bidder does not need to take bid protections into account when overbidding against other bidders at auction. In addition, a stalking horse bidder may have greater and longer access to due diligence prior to making its bid and may have a greater ability to negotiate certain terms of sale (although a 363 sale will usually be on an “as is, where is” basis).

Drawbacks to a 363 sale are that the process can be expensive and slow, every term of sale is public record, and the buyer risks being outbid at auction. Due diligence may also be limited— or at least subject to a very short review period (compared to non-distressed out of court acquisitions)—for bidders other than the stalking horse bidder.

Assignment for the Benefit of Creditors

An ABC is an insolvency proceeding under state law that can be an alternative to chapter 7 or chapter 11 bankruptcies. ABC processes vary by state—some require a court proceeding while others do not. ABCs usually require the cooperation of the debtor and its secured lender. The seller assigns its assets to a third party who is then responsible for selling the assets and distributing the proceeds to the seller's creditors. Immediately after the execution of the ABC document, the assignee takes possession of the assets. Because the buyer acquires the assets from an independent third party (the "assignee") and the sale is approved by the state court overseeing the ABC in states involving a court proceeding, the buyer likely reduces its risk that a creditor will bring a fraudulent transfer claim versus an arms’ length transaction with the seller. This is particularly true as more and more states' ABC laws allow sales to be approved "free and clear" of such claims.

Equity Receivership

A neutral third-party receiver is most often court-appointed at the request of a secured creditor who fears that its collateral will be dissipated or otherwise harmed. A receiver's powers and duties are imposed by statute and the court order appointing the receiver and may include operating the business, taking possession of property, bringing or defending actions, collecting rent or debts owed, and selling the assets of the company. If a receiver is authorized to sell the assets, it will do so under the supervision of the court. Usually, the receiver will ask the court to approve a sale procedure and then advertise the sale for several weeks in order to maximize recovery. The receiver sale process can be much less expensive and time consuming than a bankruptcy. The "art" of maximizing value out of a sale in a receivership case is to make sure the order approving the sale protects the distressed debt and asset purchaser from attacks by the company's creditors and others. Crafting an order that shields the transaction from fraudulent conveyance claims and finds that the sale is for value and the purchaser is acquiring good title in good faith should enable the purchaser to obtain unencumbered title.

UCC Article 9 Sales, Receivers, and Friendly Foreclosures

In addition to a lender's rights and remedies negotiated and incorporated into the governing loan documents that are triggered upon default by a borrower (or, sometimes, a guarantor), Article 9 of the Uniform Commercial Code governs the relationship between a debtor and its secured creditors. A secured party's remedies upon a borrower's default include the right to sell the collateral to a third party. An Article 9 sale provides the least protection from successor liability, but tends to be cheaper than a 363 sale, ABC, or receivership.

Particularly when a borrower wants to reduce liability on a personal guaranty to the secured creditor, the borrower may engage in a "friendly foreclosure." In a friendly foreclosure, the secured creditor and the seller agree the secured creditor will foreclose on the assets and transfer title to a buyer. The buyer should expect the secured creditor to sell the assets in as-is condition with few representations and warranties or indemnity. The structure of a friendly foreclosure may provide incremental protection against claims made by unsecured creditors and third parties asserting successor liability, because technically the purchaser is acquiring title from the foreclosing lender, not the distressed debtor/borrower. Again, how the notice and sale documents are drafted and the value paid in the transaction (which is truly out-of-court) are critical to assuring no later attacks by creditors (or others) asserting that the sale was not "commercially reasonable."

THE RISK OF FRAUDULENT CONVEYANCE

When a company that sold assets later files for bankruptcy, its transactions leading up to the bankruptcy filing will be scrutinized. Upon filing for bankruptcy, a trustee or, in some instances, a creditor may try to unwind a payment or asset transfer made before the bankruptcy filing under one of two fraudulent transfer theories: "actual fraud" or "constructive fraud."

To prove actual fraud, the trustee or creditor must show that the transfer was made with actual intent to hinder, delay, or defraud the company's creditors. Constructive fraud does not require any evidence of intent. Rather, constructive fraud requires the trustee or creditor to prove that the now-bankrupt company did not receive "fair consideration" or "reasonably equivalent value" for the assets and show that the bankrupt company was insolvent at the time of the asset sale, became insolvent or was left with unreasonably small capital as a result of the asset sale, or intended or believed that it would incur debts beyond its ability to pay such debts as they matured.

Practically speaking, so long as a seller receives what is determined to be a fair value in exchange for the assets, an asset sale will not be invalidated as a fraudulent conveyance, even if it is later determined that the seller was insolvent at the time of sale. Likewise, an asset sale by a solvent and adequately capitalized seller will not be invalidated as a fraudulent conveyance even if the seller did not receive fair value in exchange for the sold assets and so long as the sale did not render the seller insolvent, unreasonably capitalized or unable to pay its debts. In order to minimize fraudulent transfer risk when acquiring assets from a distressed seller in an arms' length transaction, it is advisable for the buyer to obtain a competent valuation from an independent valuation expert (i.e., not from the seller) prior to the sale and to ensure that the consideration being paid is reasonable equivalent to the value of the assets being acquired.

WHAT MAKES A "GOOD" DISTRESSED ASSET PURCHASE?

The short answer: due diligence. It is imperative to conduct proper due diligence when determining whether to buy distressed assets since it is far preferable to avoid buying liabilities by discovering them in advance than discovering them post-closing and with limited recourse against an insolvent seller. A buyer should not assume that he or she will be able to recover any losses from the seller through breach or representation or warranty claims under the contract since the seller may have limited, if any, business operations or liquidity after the sale.

a. Identify all the assets that come with the purchase, including intellectual property, client contracts, and goods.

b. Review client contracts scrupulously to determine whether they will be voided by insolvency or breached by nonperformance.

c. Ensure the fair value for every asset being purchased and evaluate the real underlying performance of the asset.

d. Determine the company's supply chain risk and the availability of, and costs associated with, using alternative sources of supply.

e. Analyze the company's potential employment law issues and compliance with relevant government health guidelines.

Buyers should consider going beyond their traditional diligence and obtain a third-party valuation of the assets being acquired and seek releases and waivers from third-parties who might have claims against the seller. Additionally, the buyer should consider requiring the seller to provide a fairness opinion in connection with the proposed transaction. Typically prepared by an investment bank, it provides an opinion as to whether the proposed sale price is fair to the seller. If the transaction is later challenged as a fraudulent conveyance, the fairness opinion will serve as evidence for the buyer that the price it paid provided the seller with reasonably equivalent value, making it difficult for the sale to be invalidated. Similarly, buyers should consider getting a solvency opinion because if the sale is challenged, the buyer can use the opinion as evidence that the seller was not insolvent at the time of the transfer.

Additionally, buyers should determine whether it makes sense to "holdback" a portion of the purchase price to be used to cover any losses to the buyer if there are breaches under the sale agreement. Absent such a holdback, if the seller were to file for bankruptcy after the sale, then any claim by the buyer under the sale agreement for indemnification or a purchase price adjustment will typically be treated as an unsecured claim after a bankruptcy filing.

Purchasing distressed assets often provides a unique opportunity to acquire property, expand your business, reach new markets or merely make a profit on the

strategic purchase of a troubled asset that can be improved and sold for a profit—but steering clear of all the landmines and pitfalls associated with such transactions, and maximizing the protections that can be obtained by and through court-approved sales requires the guidance of experienced insolvency professionals.

Ice Miller's Bankruptcy, Restructuring, and Creditors' Rights Group represents clients in a broad array of industries and can help evaluate what options might be available. If you need advice on selling or purchasing distressed assets, the attorneys at Ice Miller are available.

This publication is intended for general informational purposes only and does not and is not intended to constitute legal advice. The reader should consult with legal counsel to determine how laws or decisions discussed herein apply to the reader's specific circumstance.

***

Chelsea Abramowitz is a law clerk in Ice Miller's Business and Bankruptcy, Restructuring, and Creditors' Rights Groups (admission to the New York state bar pending). Chelsea earned her juris doctor from Fordham University School of Law and has a degree in public health from Tulane University.

Louis DeLucia is a partner in and chair of Ice Miller's Bankruptcy, Restructuring, and Creditors' Rights Group. His representation encompasses a wide range of issues, including complex Chapter 11 cases, bankruptcy and creditors' rights related litigation in state and federal courts, liquidation proceedings, receiverships, cross-border insolvency proceedings, non-judicial loan restructuring, workouts and other alternatives to the bankruptcy process, and state court asset recoveries and foreclosures.

Alyson Fiedler is a partner in Ice Miller's Bankruptcy, Restructuring, and Creditors' Rights Group. She has been involved in some of the largest and most complex bankruptcy cases in recent years, having served as counsel to creditors, creditors' committees, debtors, fiduciaries and other interested parties.

Jason Torf is a partner in Ice Miller's Bankruptcy, Restructuring, and Creditors' Rights Group. His focus is on helping companies dealing with financially troubled customers and other counterparties to maximize recovery and minimize risk.

---

[1] This publication discusses the purchase of distressed assets from an insolvent debtor or fiduciary appointed for an insolvent debtor. A separate publication will address the strategies, benefits and landmines associated with negotiating and acquiring distressed debt instruments, such as troubled loans held by institutional lenders and creditors.