Risk Assessment & Risk Management Strategy of the Defense Industrial Base Sector

Technical Report · September 2022

DOI: 10.13140/RG.2.2.15544.62720

1 author:

Brandon Alexander
American Public University
14 PUBLICATIONS **0** CITATIONS

SEE PROFILE

Risk Assessment & Risk Management Strategy of the Defense Industrial Base Sector

Brandon Alexander

American Public University

HLSS 505: Security Risk Management

September 17, 2022

Introduction

The defense industrial base (DIB) is a large sector that covers skilled craftmanship, research and development, and technological advancements to service the US Department of Defense. This key industry includes government-owned and operated sites as well as contractor operated sites owned by the government. Companies that comprise the DIB can be domestically or foreign based including the manufacturing of components and systems to service the Department of Defense (DHS, 2022). The Eisenhower administration made it clear that the DIB continues to be a strategic advantage for the United States in keeping our warfighters ready at a moments notice. Today this remains a true and logical statement to ensure our warfighters are ready for threats, foreign and domestic, including the cyberdomain (Watts, 2008).

The purpose of this paper is to explore, discuss and analyze current-day risks and vulnerabilities within the DIB. Additionally, points are noted to include vulnerabilities as well as remediation to minimize or eliminate risk. Last, will be a discussion on remediations for action to include short-term and long-term remedies for risk. The significance of this analysis will be to examine a current day snapshot of the DIB and to understand the risks that are affecting the industry today, present those risks and propose remediation to those risks. Provided the criticality of the DIB, the analysis and identification of risks is needed to help the community and taxpayer understand how risks are being mitigated. Specifically, which risks exist, why they exist and cost-effective ways to eliminate, mitigate or accept risk within acceptable parameters.

Defense Industrial Base Risk Identification

Intellectual Property Protection

One of the largest issues the DIB has is the theft of intellectual property. Foreign adversaries continue to lift technical and electronic data from DIB stakeholders that are trusted with the information. However, the pathway to understand what was compromised and how it was compromised is difficult and is often strangled by procedure, litigation holds and internal private business procedures and practices that overlap with DOD or conflict with DOD. Intellectual property (IP) is easier to steal in the modern era because of the methods used through electronic networks to funnel data through. The days of harboring paper records and large texts are gone because of cost savings. Despite the best controls on electronic media no single DIB entity is immune, even if the network is air gapped (Halber, 2016 and Berghel, 2015).

An unfortunate mistake that is made is that the assumption that the compliance with IP filings and IP law does not guarantee protection in the cyberdomain, specifically if the entities attempting to steal IP data are from an adversarial state. Domestic IP laws are only enforceable in the country where IP registration has occurred and the scope of the registration is tied to a single product or entity. Filing a patent or trademark for protection domestically does nothing regarding the theft of IP outside the boundary of the US. In fact, laws are out dated and are not keeping up speed with technology (Lui, 2011).

The issues surrounding this risk are happening for a few reasons. First, the DIB ownership is not to the government, it is to their shareholders (Baumgarten, 1996). Cybersecurity is not their first priority and frankly, it will never be. Shareholder equity by

way of the board and elected officials is the priority (Cuñat, et. al., 2012). Second is the cost, the cost to sustain a large network and combat IP threats requires large resources that may extend beyond the operating margins acceptable for the DIB company to function. Priorities including human capital and operations have to be considered in parallel with the threats that exist in IP theft, including digital methods (Radziwill & Benton, 2017).

To address these concerns DOD provides the standards of which to meet or exceed. However, these controls may not be 100% enforceable as companies battle with asset age and compliance. They have to accept risk when an information system is out of compliance to not interrupt major production efforts of when life or property is at risk. CISO and AO's provide justification on the risk that is presented, its level and the government either responds in favor or against a waiver for a given vulnerability. The issue for this places the risk in favor of IP thefts across the cyberdomain. Controls are in place for a reason and they are not to be ignored (Strohmier, et. al., 2022).

The recommendation to provide long term IP protection is to maintain a secure baseline compliant with or exceeding the recommendations prescribed by standard. Even if the standard is not written down, proactively identifying, closing and reporting the information system gap will go a long way to protect and mitigate the threat against IP. For the largest of DIB sector stakeholders' regulatory compliance needs to come by way of congress to enforce and promote such priority to prevent government information falling into the wrong hands quickly and easily (Onwubiko, 2015).

Large DIB companies have the fiscal means to make this happen and will comply if legislation dictates. Fine lines have to be drawn additionally in the contracting phase of

contract award being specifically contingent on which standards are enforced, when and for how long. Non-compliance means the contract stops until the IP protection compliance is resolved. Smaller DIB companies should take the same steps to maximize the effort taken to prevent data loss.

However, by participating in a government contract they may not be able to provide the same resources as a larger DIB compliant. However, due to the resource constraint this does not make them inadequate, rather it makes them the most vulnerable. CISA in addition to DISA need to make resources available for these smaller DIB to access when an IP gap is needed. Without warrant the availability of resources should be made swift and quicky to shore up the gaps. While the tax-payer can provide resources upfront, additional participation cost sharing should come from all of industry participants. This would be similar in solution to the FDIC insuring deposits on fiduciary accounts for member banks participating in FDIC, rather instead of voluntary it would be involuntary. This would spread out the funding and make resources available to both large and small and not based on ability to pay or size. Simple steps that are taken today go further than trying to catch up to the enemy later (Garvy, et. al, 2013).

Collaboration Minimization & Data Dependencies

DIB companies also collaborate together often on projects and in R&D efforts. The efforts usually come by way again of a contract between the government and the two DIB entities to permit interaction. In the life of a contract the effort of collaboration continues as relationships are built and products are produced for the mission (Dunne, 1995). However, collaboration exposes risk by simply allowing this activity to happen. There has to be a strike

between collaboration of data and outright data spillage. Combining data and collaborative efforts produced good products than a single entity alone. Often the product or deliverable is better when more eyes are on the product from start to end. Data dependency is another trouble spot when it comes to government owned and produced deliverables. Data can reside in the government's information system but be accessible by contractors that depend on that data or send data to it on a regular basis (Moore, 2014).

The effort to keeping a product alive is one thing but to share it across all of DIB enterprise and partners is a large risk that as to be mitigated. Only contractors and subcontractors need to participate in the data sharing needed to ensure the product or deliverable is serviced correctly. Those that are authorized need to ensure that inside of the areas of responsibilities that the data that is shared is pushed through a second set of eyes to approve the delivery to an outside entity. This can be done through procedure and contractual requirement (Gonzales, 2020 & Brown, 2009).

Considerable definition to the boundaries of what is shared and permitted and what is prohibited needs to be considered. In today's DIB what tends to happen is that larger non-disclosure agreements are executed by way of formality to jump through the loophole of what is needed to start the contract (Watts, 2008). In my twelve years of experience, Non-Disclosure Agreements (NDA) are not checked in detail and they are not updated in any way. They become stagnate and at the end of the day what holds legal basis is what was signed. An old enough NDA produces legal challenges that cannot be overcome, places taxpayer funding, the public and the government at risk through a legally binding mechanism (Chaudry, 2008).

In addition to the controls that need to be instituted for DIB companies working together, are the legal reviews and benchmarks that need to encompass such collaborative efforts (Vick, 1967). At least annually to avoid unnecessary risk product loss to competitors and to limit information sharing, a review panel consisting of the contract COR to analyze the components need to continue to collaborate. If actions and project dictates, the COR for the contract needs to provide the paperwork to ensure that efforts are verified minimized to prevent information sharing to other companies that are not authorized, or in the one off chance they need to be disclosed can approve a waiver through a GS-15 or higher. Pursing the waiver should be the exception and not the rule and can be eliminated if need be (Tews, 2017). Updating and keeping records that reflect the actual status of work can promote business growth and collaboration, level set expectations and ensure the terms of collaboration are transparent at the granular level.

Through considerable review of the data dependencies and collaborative efforts by way regular interactions allows for the risks regarding competitive advantage to be minimized. The entity that holds the contract for the government and their collaborators should be the subject matter experts in the efforts and products they are producing and by way of doing it through responsible measures (Pages, 1996). The review process built in to come to a common agreement of what needs changed on an annual basis reduces risk to the companies and retains competitive advantage while preserving NDA with the government as originally intended and within legal scope to protect legitimate business and technical needs for the government.

Supply Chain

Supply chain protection for the DIB is a very large problem and it is a growing problem recently with the COVID-19 pandemic. Private industry, including DIB were not immune from the supply chain issues that are still wreaking havoc on deliverables needed to ensure the US Defense Department is ready to continue and do the mission (Chowdhury, et. al., 2021). Historically for large DIB contracts considerable lead time and planning contracts are executed to bring materials to the job site and to ensure timely delivery to ensure contract execution remains on schedule (Apte, et. al., 2006). Over a period of a few years the US was at normal and growing economic capacity, and when the emergency orders came to shelter in place, the US economy contracted. However, DIB contracts must continue to operate as intended and decisions had to be made across the different enterprises how to wrestle with schedule, supply chain and product delivery (Melnyk, et. al., 2021).

Supply chains also have another risk besides unforeseen issues like the COVID-19 pandemic. There is additional risk placed in the DIB to ensure components are compliant with contracts that are awarded. A few examples can include components needed to make torpedoes, missile control systems, castings, information systems and even the microelectronics industry are subject to regulations. These regulatory efforts ensure and protect that components that are installed on a product meet specifications for safety, security, import/export compliance, TAA compliance, performance and cost. Not doing so weakens the deliverable and can cause system failures or a national security incident (Howell, 2005 and Cook, et.al, 2012).

Adequate supply chain risk management needs to continue to be strengthened across industry and suppliers providing materials for eventual government furnished and owned equipment. Adequate controls in a detailed supply chain risk management need to have their own ground to stand on. The identification of microelectronics as an example have components that are manufactured abroad. It is known that microelectronics contain backdoors inserted into them to bypass any system security that may be present. Additionally, materials for construction can be presented as satisfactory when they are delivered but are sub-par at best (VanEtten, 2016).

The single best method to ensure components meet specification before they are installed in critical areas is to have an in-house laboratory test them. The government sets certain specifications for materials that are used in critical applications. Those materials need to be independently verified in house to ensure that what comes in the door, is what is installed. Adding in the analysis time and engineering time needed to ensure these products make it to their destination is one aspect to control supply chain issues (Tate, et. al., 2014).

In addition to in-house laboratory testing, quality inspectors forming a solid line of receipt inspection to verify components for cleanliness and free from damage (Azamfirei, et. al, 2021). This is another solution to mitigate the risk of installing a faulty part or item that was manufactured into a missile or torpedo for example. The part may meet laboratory specifications but if it is bent or damaged that part can cause issues. Multiple layers of plant wide inspection and audit to provide historical re-construction helps in the event of an accident or issue. While no process exists in a vacuum, adding these two critical aspects into the supply chain, reduces risks of outside components causing trouble in DIB built critical systems.

Human Capital Risk & Security Clearance

The DIB touches and services most areas in the Department of Defense. Many of the components and products that go into the use and manufacturing rely on a trusted workforce. In the present day human capital continues to be a risk of both positive and negative within in the DIB sector. The business of defense cannot be done without human capital. The processes needed to protect current the current workforce and the future workforce have to be considered and risk mitigated. To focus on the critical nature of the work the DIB sector does, DIB entities recruit talent from across the nation to perform this type of work (Schuler, 1989).

Career analysis is performed to ensure they attract the right talent but also retain that talent for the long term (Callaway, 2007). Incentives today are paving the way for the DIB to ensure they have the human capital needed to survive the economy in a now near post COVID-19 environment. Manufacturing sectors of the DIB now are offering referral and sign on bonuses to those that join the team successfully (Dial & Murphy, 1995). One issue with this is that the current employee base does not enjoy the benefits of getting a $5,000 sign on bonus when no bonus was offered when they signed on decades ago. This affects morale and may cause talent to leave for greener pastures, not only to claim the new bonuses but to garner a higher salary in most cases.

Secondary to talent retention comes that of a trusted workforce. By the way of the security clearance process those that wish to work in the sensitive sector of the DIB industry have to obtain and maintain a clearance of that to which they are working or are anticipating on working. Candidates are turned down for financial irresponsibility, DUI, criminal activities, drug use and risky behaviors as determined by an adjudicator (Goldstein, 1991 &

Lebowitz, 2019). While the candidates turned down are not given a reason for the failure, the results are often clear when the rejection comes (Brown, et. al, 2020 & Lebowitz, 2019).By way of the adjudication and vetting process millions of applicants and thousands of potential employees are reduced down to an acceptable pool to ensure the interests of nations security are protected. If those interests are not protected, entire DIB programs are at risk as well being barred from future contract activities (Gallagher, 1983).

While necessary to retain talent the risk of not having human capital are astronomical considering how large the DIB sector is. The risk is simple but complex, high value for high risk; but is the risk worth the reward. Many DIB component managers look favorably when a security clearance process has passed and a new employee that has been minted joins the ranks to participate in this industry. However, the opposite is true, while a candidate may not qualify for a security clearance initially one could be granted by way of appeal (Patel, 201)

The solution to retain talent needs to start within. To mitigate the risk of the current workforce leaving, additional or the same bonuses need to be offered to those on the workforce and that have been on the job for over ten years. This is both an adequate test of time and fidelity to ensure they stay on the job and do not leave. This is a simple task and requires budgetary approval to have payroll pass the deposit on to the employee. The current workforce that is getting the new bonuses should sign a non-compete contract as well as a long-term contract to ensure they stay long enough to cover the initial monetary award. A fair estimate would be for every $1,000 one year is required or the award has to be returned in the entirety.

The security clearance helps reduce risk to the DIB sector to ensure the workforce is trusted. However, this is not a sealed deal as those with security clearances have wreaked havoc inside of government programs and within the government over the past decade. Edward Snowden was a contractor for BAH for a number of years and still exported classified information at the TS level to Singapore. This is a serious problem and a serious failure of oversight when the security clearance system should have flagged him as a risk to begin with and terminate his clearance when issues arrived. The solution to this risk and to increase national security is to provide up to date clearance and vetting factors to candidates that participate in the DIB sector (Brody & Cox, 2015 and Anderson, 2022).

The system we have today is just now migrating to Continuous Evaluation/Continuous Vetting but the entire government has not arrived at a single consensus of how soon they need to arrive on shore. The process of CE/CV needs sped up and to meet the demand of detecting incidents before they happen. If this cannot be done in a reasonable time, then a new system needs developed to replace the outbound one. Either way time and security are of great magnitude, considering the mission of the US Department of Defense. Eventually having a system that keeps up with low-level trends can reduce incidents from happening and suspending classified access before an incident happens (Doubleday, 2017; Farrell, 2018; Farrell, 2017).

Providing a secure and steady workforce is extremely important considering the evolving threat that is at the door steps of the Department of Defense and also DIB sector activities throughout the nation. The process of improving human capital and reducing risk through incentive and a new clearance adjudication program will renew and strengthen the

DIB plus provide worker satisfaction in the renewed effort of retaining them for the long term.

Physical security/asset management

Much goes by the way of physical security of the DIB sector. Physical security is what the general public interfaces with when a visit is needed or warranted. Specific controls are needed to ensure the correct individuals and people make it to the DIB sector site without impeding the courses of day-to-day activities. For obvious reasons people off of the street and the general public cannot walk into a defense installation and the same is true for the DIB sector installations. Strong but necessary physical security is needed to mitigate physical risks from interrupting the products that flow from the DIB sector. Photographs can be taken and shared across the world in a few seconds, access to dangerous work areas and improper admittance without a security clearance would allow people to view state secrets unchallenged. This leads to a degrade in a competitive edge across the DIB sector and would introduce unnecessary risk of the public entering these facilities at the risk of the DIB sector component (Clapper, 2009).

Improving physical security happened by way of HSPD-12; this made the identification of contractors and civilians universal across government (Bush, 2004). However not all DIB sectors comply with HSPD-12 to provide this identification measure. As private industry sectors, adding the CAC/PIV credential to every staff member would not be cost effect to manage as well as have updates to the credential when needed. This effort would cause work stoppage and long lines at security offices of which only a few PIV/CAC issuance stations operate. Rather they utilize a simpler solution, often internal to the company to

provide credentialing that is more manageable and solution oriented to control physical access. However, this does come with significant risk and that risk has to be accepted and controlled (Carter & Rilett, 2022 and Clapper, 2009).

One issue with physical access is that of entry control. The card has to be on that person. Inside the DIB facility this is fine, however outside this is problematic. The physical identification contains the picture, name and identifying information about the employee. These cards can be duplicated because they are commercially available and the equipment to make them is available off the shelf. The cost of physical cards are inexpensive, pennies when ordered in the thousands. They are also subject to RFID attack and spoofing if these technologies are included. The management of a large number of credentials becomes challenging because the risk of loss or theft is high since the physical cost of the cards are low. A more robust solution needs to be developed to enable the DIB sector to match that of HSPD-12. (Bush, 2004 & Geldenhuys, 2016).

The requirements of HSPD-12 can be cumbersome for industry however continuing on the way ahead of today has to cease. State actors are smarter and more intelligent that what is perceived. The logical control starts at the gate of the DIB facility. Security forces are the front line to verify the authenticity of issued credentials. When the electronic system goes down, hand verification is required. Admitting someone who should not be admitted is a problem and denying entry to someone who has legitimate access is also a problem.

The solution to this is to provide a balance to coming close to HSPD-12 but operate within the boundaries of NISPOM requirements (Barr, et. al., 2008). A significant improvement over the commercial off the shelf solutions for identity protection needs to be in

place. Most DIB facilities have an internal department that handles credentialing but the facilities need upgraded to encompass a higher fidelity of protection regarding physical access. DIB facilities have logs that the visitor signs and validation is performed usually on the spot through hard media verification (Driver license, passport, birth certificate). No other biometric data is captured other than the signature in most cases.

With HSPD-12 issuance biometric data is collected and verified with hard data. Collection, verification and storage along with the establishment of a PIN is stored in a database and verified against other interconnected databases to ensure the identity of the person matches the biometric identification. As a multi factor approach, this method is more secure and requires infrastructure to support it (Bush, 2004).

A solution for DIB to incorporate could be a simple as adding a PIN to the card or issuing a tamper resistant card holder can mitigate RFID attacks. Additional layering can come later as physical security warrants with time (Archana, et. al, 2017). Having this simple solution is cost effective and simple and provides employees without clearances the same protection as those with. Since clearances can only be verified with DISS (formally JPAS) or Scattered Castles, those without clearances have no formal vetting at this level. This level of effort can provide those with and without clearance physical access to the DIB facility with minimal interruption.

Recommendations/Conclusion

The mitigation of the risks identified above can be remedied by changing or institution current practices to make the more efficient, effective and impactful to the DIB sector. To minimize risks logical and meaningful steps need to be taken to ensure guidelines are

followed regarding any issues relating to the product or deliverable specific DIB sectors are producing. These products are going to be unique but they all service the Department of Defense (Watts, 2008).

A common understanding and implementation of simple steps can dramatically improve aspects that surround the current challenges facing the DIB sector. Change can be difficult and there is also the issue of workplace culture that remains challenging to change. In instances, cells of older workforce members do not want to change the practices that have been in place for long periods of time. The mantra of "it worked then; it will work now"; is not acceptable. Transparently speaking this is the unequivocal definition complacency. Our adversaries work just as hard to steal data and thwart controls to access facilities as we do building it. Attacks against the DIB sector continue to be and are on the rise. Those attacks can lead to loss of life and property if risks are left unchecked or are stale. All of us, DIB sector employees and government employees will need to rely on the DIB sector to transform business practices to reduce and eliminate risk across the board. Doing so will only strengthen our national security.

References

Anderson, P. D. (2022). On Moderate and Radical Government Whistleblowing: Edward Snowden and Julian Assange as Theorists of Whistleblowing Ethics. *Journal of Media Ethics*, *37*(1), 38-52.

Apte, U., Ferrer, G., Lewis, I., & Rendon, R. (2006). Managing the service supply chain in the Department of Defense: Opportunities and challenges.

Archana, B. S., Chandrashekar, A., Bangi, A. G., Sanjana, B. M., & Akram, S. (2017, May). Survey on usable and secure two-factor authentication. In *2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT)* (pp. 842-846). IEEE.

Azamfirei, V., Granlund, A., & Lagrosen, Y. (2021). Multi-layer quality inspection system framework for industry 4.0. *International journal of automation technology*, *15*(5), 641-650.

Barr, A. C., Denomme, T. J., Booth, B., Krump, J., Sloan, K., Slodkowski, L., & Sterling, S. (2008). *Department of Defense: Observations on the National Industrial Security Program*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Baumgarten, L. (1996). The Transformation of Ownership Relations in Defense Industries Privatization of defense industry enterprises. *Problems of Economic Transition*, *39*(7), 44-59.

Berghel, H. (2015). A farewell to air gaps, part 1. *Computer*, *48*(6), 64-68.

Brody, R. G., & Cox, V. L. (2015). Background investigations a comparative analysis of background checks and federal security clearance investigations. *Business Studies Journal*, *7*(1).

Brown, R. A., Yeung, D., Gehlhaus, D., & O'Connor, K. (2020). *Corporate Knowledge for Government Decisionmakers: Insights on Screening, Vetting, and Monitoring Processes*. RAND Corporation.

Brown, T. A. (2009). Legal propriety of protecting defense industrial base information infrastructure. *AFL Rev.*, *64*, 211.

Bush, G. W. (2004). Homeland security presidential directive/Hspd-12. *Retrieved on Jan*, *10*, 2008.

Callaway, P. (2007). *The relationship of organizational trust and job satisfaction: An analysis in the US federal work force*. Universal-Publishers.

Carter, S. D., & Rilett, L. R. (2022). Evaluation of Department of Defense Installation Entry Control Facilities Using Microsimulation. *Transportation Research Record*, 03611981221114116.

Chaudhry, R., & Kamei, K. G. (2008). Can Your Firm Keep Its Secrets. *No. 181 Managing Intell. Prop.*, 109.

Chowdhury, P., Paul, S. K., Kaisar, S., & Moktadir, M. A. (2021). COVID-19 pandemic related supply chain studies: A systematic review. *Transportation Research Part E: Logistics and Transportation Review*, *148*, 102271.

Clapper Jr, J. R. (2009). *DoD IG Report to Congress on Section 357 of the National Defense Authorization Act for Fiscal Year 2008. Review of Physical Security of DoD Installations*. INSPECTOR GENERAL DEPT OF DEFENSE ARLINGTON VA.

Cook, T., Alston, R., & Raia, K. (2012). *Mastering Import and export management*. Amacom.

Cuñat, V., Gine, M., & Guadalupe, M. (2012). The vote is cast: The effect of corporate governance on shareholder value. *The journal of finance*, *67*(5), 1943-1977.

DHS, (2022). Defense Industrial Base Sector-CISA. Retrieved 16 September 2022, from https://www.cisa.gov/defense-industrial-base-sector.

Dial, J., & Murphy, K. J. (1995). Incentives, downsizing, and value creation at General Dynamics. *Journal of Financial Economics*, *37*(3), 261-314.

Doubleday, J. (2017). Lawmakers seek to let DOD take over security clearance investigations. *Inside the Pentagon*, *33*(28), 1-8.

Dunne, J. P. (1995). The defense industrial base. *Handbook of defense economics*, *1*, 399-430.

Farrell, B. S. (2017). *Personnel Security Clearances: Additional Actions Needed to Ensure Quality, Address Timeliness, and Reduce Investigation Backlog*. United States Government Accountability Office.

Farrell, B. S. (2018). *Personnel Security Clearances Additional Actions Needed to Implement Key Reforms and Improve Timely Processing of Investigations*. United States Government Accountability Office.

Gallagher, M. G. (1983). Defense of Adverse Actions against Federal Civilian Employees Occasioned by the Revocation of a Security Clearance. *Army Law.*, 18.

Garvey, P. R., Moynihan, R. A., & Servi, L. (2013). A macro method for measuring economic-benefit returns on cybersecurity investments: The table top approach. *Systems Engineering*, *16*(3), 313-328.

Geldenhuys, N. D. (2016). *An evaluation of identification methods used in the investigation of counterfeit card fraud* (Doctoral dissertation).

Goldstein, J. G. (1991). *Financial Criteria Used in Case Adjudication by the Directorate for Industrial Security Clearance Review (DISCR)*. NAVAL POSTGRADUATE SCHOOL MONTEREY CA.

Gonzales, D., Harting, S., Adgie, M. K., Brackup, J., Polley, L., & Stanley, K. D. (2020). *Unclassified and secure: a defense industrial base cyber protection program for unclassified defense networks*. RAND Arroyo Center Santa Monica CA, Santa Monica United States.

Halbert, D. (2016). Intellectual property theft and national security: Agendas and assumptions. *The Information Society*, *32*(4), 256-268.

Howell, J. A. (2005). The Trade Agreements Act of 1979 Versus the Buy American Act: The Irresistible Force Meets the Immovable Object. *Pub. Cont. LJ*, *35*, 495.

Lebowitz, M. J. (2019). The Enigmatic Adjudicator: A Brief Primer on the DoD CAF Process. *Army Law.*, 26.

Lui, C. (2011). Navigating through the legal minefield of state and federal filing for perfecting security interests in intellectual property. *Santa Clara L. Rev.*, *51*, 705.

Melnyk, S. A., Schoenherr, T., Verter, V., Evans, C., & Shanley, C. (2021). The pandemic and SME supply chains: Learning from early experiences of SME suppliers in the US defense industry. *Journal of Purchasing and Supply Management*, *27*(4), 100714.

Moore, N. Y., Grammich, C. A., & Mele, J. D. (2014). *Findings from existing data on the Department of Defense industrial base*. RAND National Defense Research Inst. Santa Monica CA.

Onwubiko, C. (2015. Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. In *2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)* (pp. 1-10). IEEE.

Pages, E. R. (1996). *Responding to Defense Dependence: Policy Ideas and the American Defense Industrial Base*. Greenwood Publishing Group.

Patel, N. A. (2011). You're Fired! Egan and MSPB Review of Security Clearance Decisions. *Fed. Cir. BJ*, *21*, 93.

Radziwill, N. M., & Benton, M. C. (2017). Cybersecurity cost of quality: Managing the costs of cybersecurity risk management. *arXiv preprint arXiv:1707.02653*.

Schuler, R. S. (1989). Strategic human resource management and industrial relations. *Human relations*, *42*(2), 157-184.

Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J., & Modaresnezhad, M. (2022). Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base. *Journal of Information Systems Applied Research*.

Tate, J. R., Johnson, R., Barth, J., & Panteghini, M. (2014). Harmonization of laboratory testing—current achievements and future strategies. *Clinica Chimica Acta*, *432*, 4-7.

Tewes, J. (2017). Cybersecurity as airworthiness. *Available at SSRN 3033898*.

Van Etten, S. R. (2016). *Cyber Supply Chain Security: Can The Backdoor Be Closed With Trusted Design, Manufacturing And Supply*. Air Command and Staff, Air University Maxwell AFB United States.

Vick, W. O. (1967). Role of Defense Contract Audit Agency under PL 87-653. *Pub. Cont. LJ*, *1*, 58.

Watts, B. (2008). *The US Defense Industrial Base: Past, Present and Future* [Ebook]. CBSA. Retrieved 16 September 2022, from https://csbaonline.org/research/publications/the-us-defense-industrial-base-past-present-and-future/publication/1.