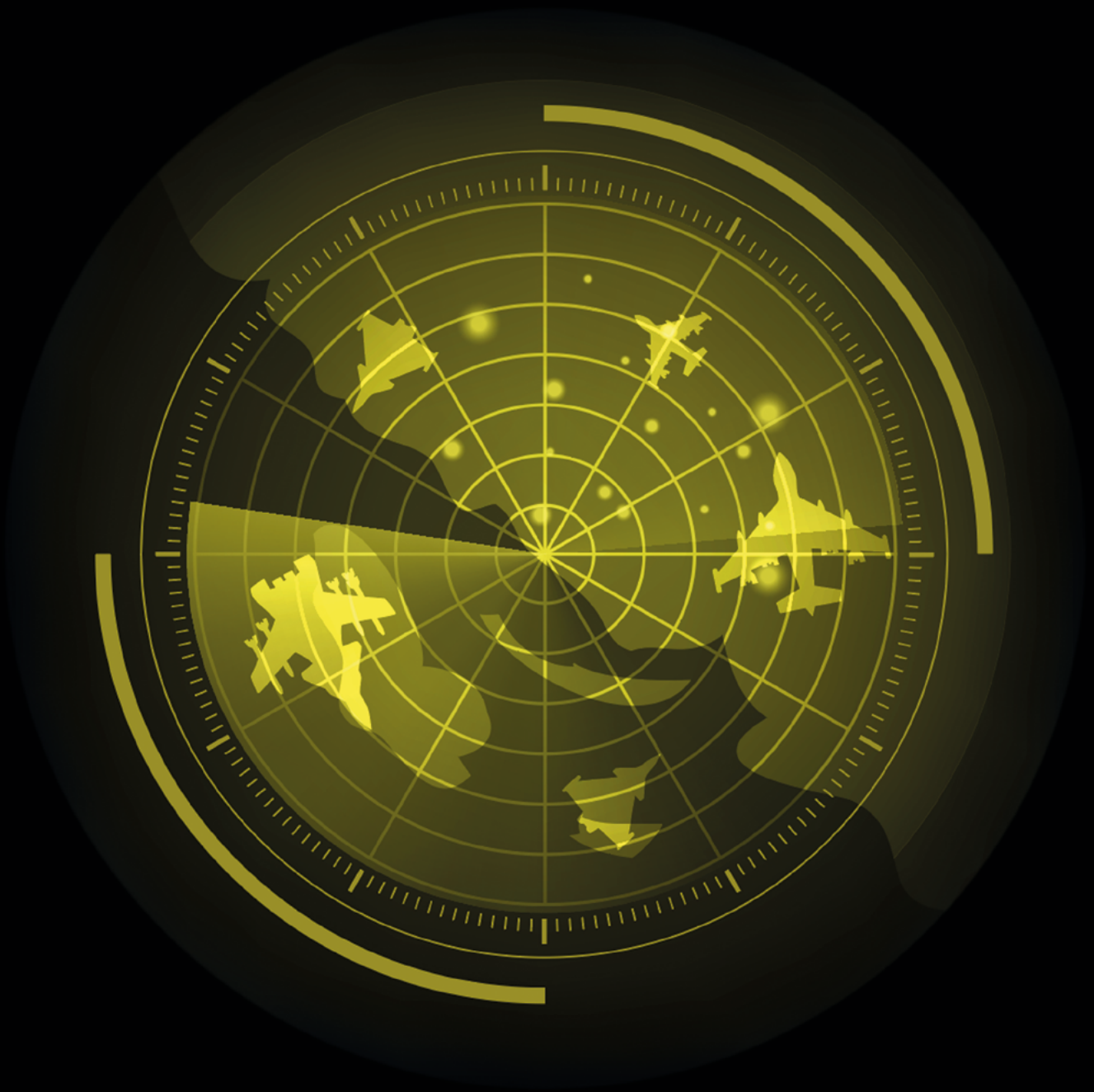
Deloitte.



Third-party risk management

Cybersecurity in the Defense Industrial Base (DIB)

Contents

Executive summary

Supply chain attacks, which exploit security weaknesses in third-party services to strike a target, increased 78 percent between 2017 and 2018 according to Symantec's 2019 Internet Security Threat Report, and the trend is increasing in 2019.[1] As the potential for these types of attacks continues to grow, defense industry affiliates will need to look beyond the minimum requirements within the self-reported compliance checklist and build a proactive, broader approach to managing risks within their enterprises. This approach should include formalized policies and the identification of patterns and practices mapped to existing Department of Defense (DoD) requirements to assess supply chain risks and better manage potential supply chain vulnerabilities.

Defense Industrial Base (DIB) affiliates, encompassing global supply and logistics chains, can have a connection to the DIB network and have access to sensitive or classified technologies and information. Cyber is everywhere, and as attackers continue to look for new entry points, these affiliates are increasingly becoming more susceptible to espionage and may be a target for theft and sabotage where counterfeit or otherwise faulty components could enter the supply chain. These threats are amplified by the complexity of modern supply chains, which may include foreign entities, bringing concerns of "upstream" targeting. The globalization and virtualization of the business landscape presents new challenges to ensuring risk management of national security interest programs and associated information systems' components and information.

Defense contractors are increasingly investing in digital technologies to help accelerate product development, improve existing processes, and increase efficiency. Digitization results in highly sensitive and confidential data being stored long term and shared internally as well as externally. Defense contractors have a heightened responsibility to protect this data in its digital form so as to not negate the benefits. National security concerns elevate the importance of data security for defense contractors. They share, exchange, and create Covered Defense Information (CDI) and Controlled Unclassified Information (CUI) on program specifications, technology, and equipment performance as they collaborate across research, design, development, and deployment of defense products. Apart from a national security threat, cyberattacks can also cause significant financial and reputational damage to defense contractors, which may disrupt supply chains and result in cost and schedule overruns.

DIB third-party risk management strategy

1. It is imperative that defense contractors be well prepared to manage cybersecurity risks within their supply chain to protect against national security threats.
2. To prepare for the future, DoD prime contractors and suppliers should consider integrating a supply chain cyber governance program that clearly maps out the steps to be compliant and cyber resilient.
3. Consider leveraging emerging technologies such as digital process automation, blockchain technology, artificial intelligence, and advanced analytics to scale illumination and prioritization of high-risk third parties across the DIB.

The US governing authorities have issued several regulations related to cybersecurity compliance by defense contractors and subcontractors. Initially, there seemed to be some ambiguity in determining who is accountable and responsible across the DIB for evaluating suppliers' adherence with the requirements in the National Institute of Standards and Technology (NIST) SP 800-171.[2] This approach allowed for the possibility of inconsistent adoption of these regulations; however, with a recent announcement by the Office of the Secretary of Defense, the DoD is now moving to enforce compliance with the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012,[3] including the cybersecurity flow-down requirements.

In this article, we will explore some of the major challenges related to cybersecurity regulations for defense contractors in the supply chain risk management domain. We will also define steps key stakeholders should consider in becoming compliant with regulations enforced by the DoD and ideas to make progress toward a more cyber-resilient security posture.

Background

Stakes are high for DIB affiliates who provide research and development, manufacturing, mission assurance, engineering, logistics and acquisition, cybersecurity and IT, and testing and integration services.

DIB affiliates are constantly innovating to produce technologically advanced products, and the speed of innovation results in creating a significant amount of intellectual property (IP), which must be digitally protected by all participants in the supply chain. The risk of aggregated CDI and CUI with respect to future defense capabilities or IP being exposed to cyberattacks is a major threat to the national security of the United States.

Defense manufacturing often involves a complex global supply chain, involving tier-1, tier-2, and tier-3 contractors. This complexity introduces numerous cybersecurity risks as the involvement of multiple organizations places confidential information in environments with greater opportunity for compromise and exploitation. Moving further down the supply chain, lower-tier suppliers generally face even more difficulties to secure sensitive data because of costly, inconsistent, or incompatible cybersecurity controls implementations or from a misinterpretation of the required regulations.

The United States has faced numerous and varied cybersecurity threats in the past, which have involved attempts at infiltrating the networks of US public and private institutions, to gain access to sensitive information.[4] If the defense manufacturing supply chain is vulnerable to cyberattacks such as counterfeit parts insertion, corporate espionage, IP theft, network compromise, foreign influence, etc., it can pose major risks that may compromise a nation's safety:

- IP theft by hostile nations or terrorist groups to advance defense capabilities, develop more effective countermeasures, produce technologies for sale on the global arms market, and erode US military superiority
- Data theft to monitor and possibly infiltrate defense systems and capabilities, thus reducing the lethality of military tactics

Level of perceived cybersecurity risks highest for information technology (IT)/IP and business system threats

In a study titled "Implementing Cybersecurity in DoD Supply Chains," the National Defense Industrial Association (NDIA) conducted a survey of 227 NDIA members engaged in the manufacturing or supply of components and services to the DoD to assess the apparent risks of three dimensions of cybersecurity threats that defense contractors face: IT/IP threats, business system threats, and factory/shop floor threats.

The level of perceived cybersecurity risks by defense contractors was the highest with respect to IT/IP threats, where 87 percent of respondents believed the risks to be either "high" or "extremely high." This was followed by business system threats, where 76 percent of respondents perceived the risks to be high.

The level of cybersecurity investment correlated with the attitude toward the perceived level of risk as most of the respondents designated greater importance to IT/IP and business system threats.

Source: Steven A. Melnyk, Chris Peters, Joseph Spruill, and Kenneth W. Sullivan, *Implementing cybersecurity in DoD supply chains,* NDIA, July 2018, http://www.ndia.org/-/media/sites/ndia/divisions/manufacturing/documents/cybersecurity-in-dod-supply-chains.ashx?la=en.

In 2018, cybercriminals hacked into a US Navy contractor's system to steal data on plans to build an anti-ship missile by 2020 for use on US submarines. Hackers breached the systems of the contractor and stole sensitive data related to sensors, cryptographic information, the electronic warfare library of the Navy, and information on a secret project named "Sea Dragon."

Source: Ellen Nakashima and Paul Sonne, "China hacked a Navy contractor and secured a trove of highly sensitive data on submarine warfare," *The Washington Post,* June 8, 2018, https://www.washingtonpost.com/world/national-security/china-hacked-a-navy-contractor-and-secured-a-trove-of-highly-sensitive-data-on-submarine-warfare/2018/06/08/6cc396fa-68e6-11e8-bea7-c8eb28bc52b1_story.html?utm_term=.0499ebf4afdd.

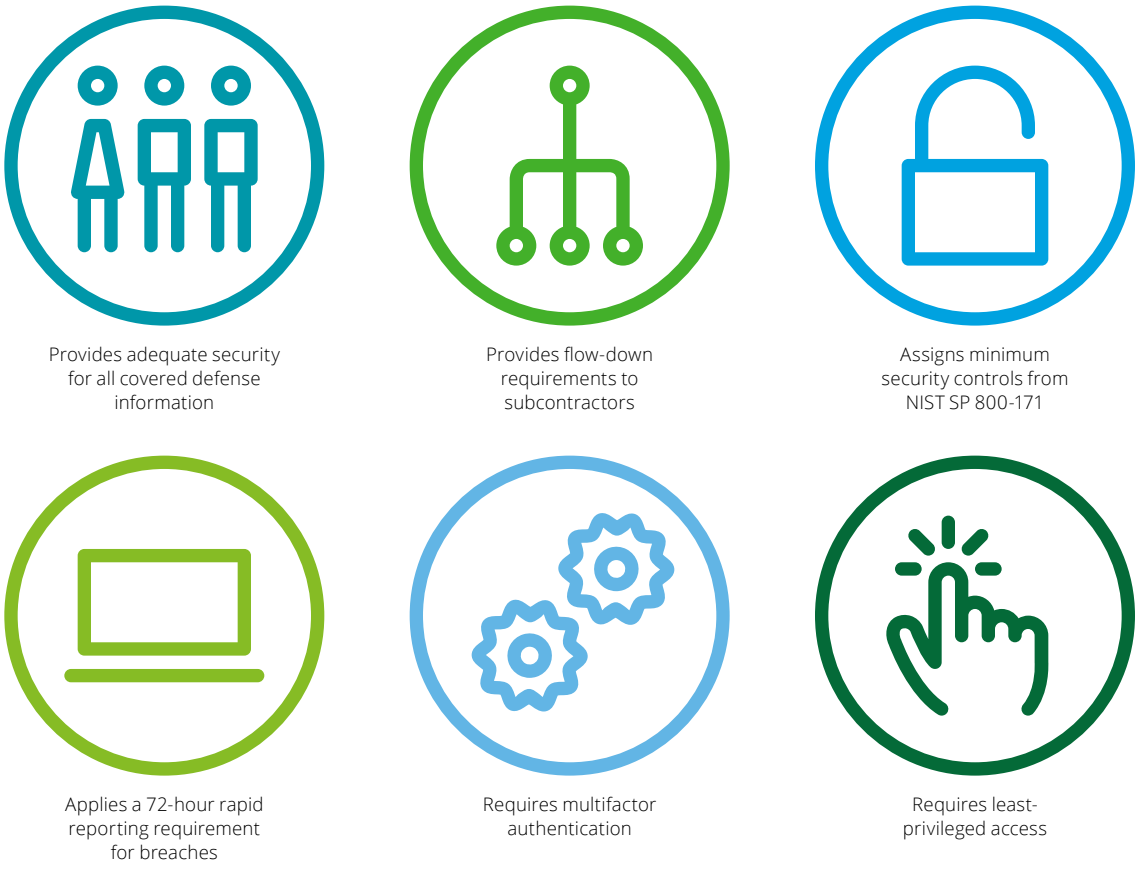
Current regulation and guidance

DFARS regulations and NIST guidance play an important role in the United States to enable cybersecurity robustness. For defense contractors and subcontractors, regulations can provide a minimum guidance to assist them with becoming cybersecure, as referenced in figure 1 and described below:

- In the United States, the DFARS requirements and compliance with the NIST SP 800-171 govern the DIB and associated contractors.[5] The DFARS 204.7300[6] requires contractors and subcontractors to protect CDI by applying specified network security requirements and necessitates reporting of cyber incidents. DFARS 252.204-7012[7] further expands the definition of CUI and identifies the NIST SP 800-171 framework as a source document for cybersecurity requirements.
- NIST SP 800-171, which lays down specific measures to safeguard sensitive information, acts as a minimum standard for companies in the DIB.

To provide guidance for implementation and enforcement of DFARS, a report by The MITRE Corporation was published in August 2018, which advised the DoD to "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."[8]

Figure 1. DFARS base clause requirements for defense contractors



Source: Deloitte analysis of DFARS regulation.

Challenges with regulation and guidance adoption

Significant importance is being given to cybersecurity because of a robust regulatory system. However, these regulations will need to be clearly defined to avoid straining defense contractors in their adoption and implementation, and to help avoid unidentified risks. Defense contractors and their suppliers in the United States face various challenges when it comes to adhering to cybersecurity regulations (see figure 2).

Figure 2. Current regulations can pose a challenge for prime contractors

Source: Deloitte analysis.

1. Regulations have not fully clarified the degree to which prime contractors should verify cyber compliance throughout the supply chain. Until recently, the DFARS required that defense prime contractors contractually "flow down" the responsibility to comply with NIST SP 800-171 to subcontractors. Unfortunately, no formal governance program was established to assess risk and enforce compliance throughout the supply chain.
2. DoD prime contractors do not typically verify suppliers' compliance with NIST SP 800-171. This is especially true for small- and medium-sized contractors. Moreover, it is becoming increasingly difficult and costly for prime contractors to understand and manage the risks of multiple subcontractors.
3. Small- and medium-sized defense contractors face several issues with respect to regulatory compliance, including awareness and full understanding of the compliance regulations and the lack of financial resources to establish broad-reaching governance programs.
4. The DIB cybersecurity information sharing program provides for mandatory reporting on cybersecurity incidents, but much of the nonreporting requirements remain voluntary; widespread dissemination of threat information could potentially benefit lower-tier contractors and provide improved situational awareness throughout the sector.

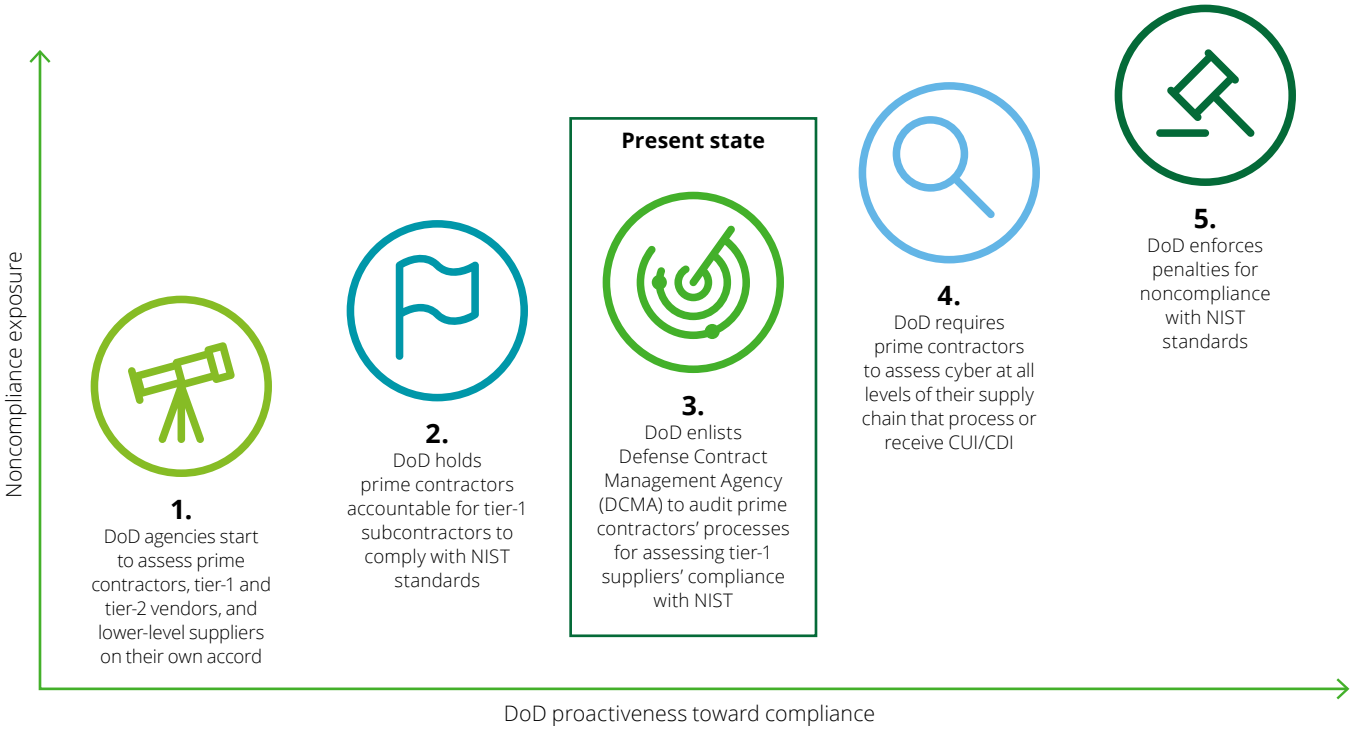
Regulatory requirement challenges and noncompliance could drive the DoD to intervene and take the necessary steps to achieve compliance, which may include stricter actions, based on the severity of noncompliance. If the DoD observes that the industry is slow at adopting these regulations, they may consider taking incremental steps, which could be a wide range of options, including risk assessing the contractors and their subcontractors, holding prime contractors accountable for noncompliance across the DIB, or continuous monitoring of high-risk DIB partners.

Government response

DoD agencies are taking various steps to understand the level of compliance of the supply chain on their programs to NIST SP 800-171. While certain DoD agencies are assessing or "auditing" the prime contractors' compliance with the DFARS standards, some of them are also assessing the compliance to NIST SP 800-171 of the lower-tier suppliers in their supply chain. All these efforts are helping the DoD form an understanding as to the level of adoption in the industry (see figure 3).

According to a report from the DoD Inspector General (DoDIG) released in March 2018, the DoD conducted an audit focused on cybersecurity controls at seven Missile Defense Agency (MDA) contractor facilities. The audit revealed that these "MDA contractors did not consistently implement security controls and processes to protect classified and unclassified ballistic missile defense system (BMDS) technical information." The DoD's increased enforcement of DFARS flow-down requirements is evidenced by the DoDIG report, which was critical of a DoD agency for not aggressively ensuring all its suppliers complied with the NIST SP 800-171 and for not making enough progress on a Plan of Actions and Milestones (POA&M) put in place to address these vulnerabilities.[9]

Figure 3. The extent to which the DoD could go to address noncompliance



Source: Deloitte analysis.

Defense prime contractors now have an increased responsibility toward achieving compliance

The DoD has recently clarified the direction in which it plans to move to drive greater NIST adoption down into the DIB. On January 21, 2019, Under Secretary of Defense for Acquisition and Sustainment Ellen Lord issued a memorandum requesting the DCMA to validate prime contractors' compliance with DFARS 252.204-7012.[10] The memorandum focused on the DCMA assessing two key elements:

- Ensuring contract terms flow down to tier-1 level suppliers correctly
- Reviewing prime contractors' procedures to assess compliance of their tier-1 level suppliers with DFARS 252.204-7012 and NIST SP 800-171

Subsequently, on February 26, 2019, the DCMA officially updated its Contractor Purchasing System Review (CPSR) Guidebook to include new procedures for its procurement analysts to assess the two aspects stated in the memo issued by Ellen Lord.[11] Specifically, it stipulated that:

"The prime contractor must validate that the subcontractor has a Covered Contractor Information System (CCIS) that can receive and protect CUI. The prime contractor must show documentation that they have determined that the subcontractor has an acceptable CCIS to include an adequate System Security Plan (SSP)."

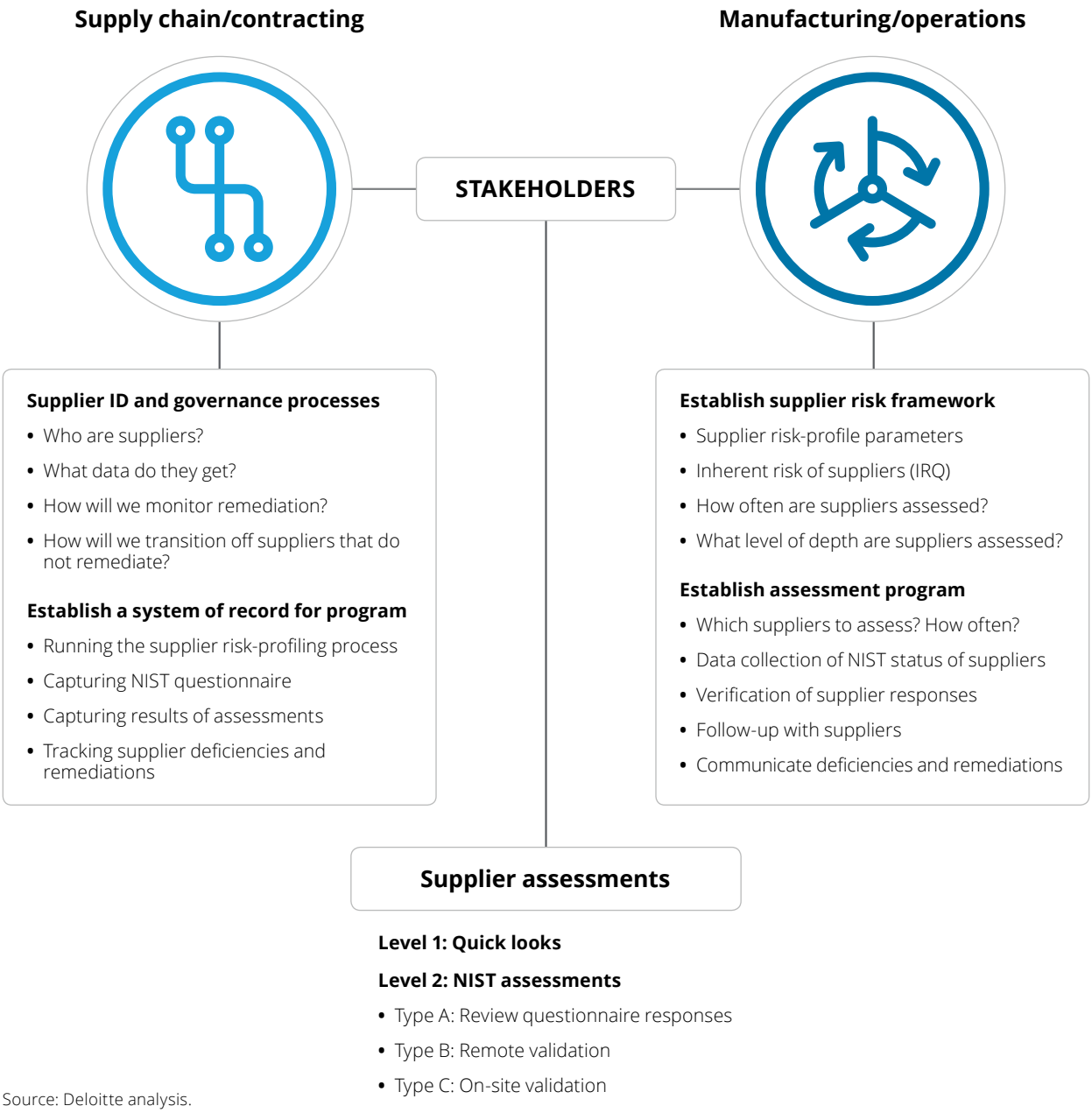
These steps assist the prime contractors to have a process to assess and validate the cyber controls a contractor has in place and to address, at a minimum, the NIST SP 800-171 requirements and that items that were identified in previous POA&Ms are being resolved as part of their self-certifications.

Taking a cybersecurity framework approach to manage requirements

As the DoD starts to enforce evaluation of subcontractors' cybersecurity controls by the DoD prime contractors, there are several measures that defense contractors, the DoD, and the government can take to become cyber resilient and compliant.

Prime contractors and original equipment manufacturers (OEMs) should focus on creating a robust cybersecurity framework, both to protect their own and their supply chain partners' cybersecurity. To be prepared, defense contractors should focus on both regulatory and nonregulatory approaches to addressing cybersecurity issues.

Figure 4. Supply chain governance program



Source: Deloitte analysis.

From a regulatory compliance perspective, prime contractors should migrate toward a supply chain cyber governance program based around NIST SP 800-171. First, DoD prime contractors should have processes in place to continually assess their own companies' compliance with NIST SP 800-171 controls and the progress of action plans for improvement. Second, they should create awareness among subcontractors and small- and medium-sized suppliers as to what NIST SP 800-171 compliance means. For instance, providing training and education to the chief information security officers (CISOs) of subcontractors and realistic solution options that can help demystify what it takes to provide adequate cybersecurity for small- and medium-sized suppliers. Lastly, DoD prime contractors should take steps to demonstrate initiative in taking responsibility for the flow down of NIST SP 800-171 compliance requirements to their supplier ecosystem—for example, creating a third-party cyber assessment program or performing regular cybersecurity evaluations of their suppliers to improve confidence that the supply chain is well prepared for cybersecurity risks and is making progress on their POA&M.

To prepare for the new cybersecurity flow-down procedures and the DCMA's upcoming CPSRs, integrating a supply chain cyber governance program as depicted in figure 4 could potentially help improve compliance, both within the organization and by their suppliers.

- **Illuminate the ecosystem of suppliers on your defense programs:** Conduct a due-diligence discovery of suppliers using a detailed survey combined with a passive Open Source illumination to identify the suppliers that are in the supply chain ecosystem. While the DCMA is currently looking to evaluate prime contractors' assessments of their tier-1 suppliers, this should go down to tier-5 suppliers at a minimum, depending on the criticality of the program and how far down CDI flows in the supply chain.

- **Risk rank the criticality of those suppliers:** To ensure the right assessment approach is applied to the right suppliers, organizations can consider using risk-ranking criteria to rank the suppliers in risk tiers. Risk-ranking factors could include CDI exposure, company reputation, company size, financial stability, foreign influence, foreign operating locations, corporate leadership, cyber breach history, the importance of their role in the DoD program, etc.
- **Identify the riskiest suppliers and assess the extent of their exposure:** Adjust the approaches for assessing NIST SP 800-171 compliance to the risk tier of the supplier. For the highest-risk tier suppliers, prime contractors should consider on-site validation of cybersecurity controls, whereas, for lower-risk tiers, options such as passive cybersecurity noncompliance evaluation, or short-term adversarial assessments using advanced analytics to determine basic cyber hygiene can be considered.

Additional nonregulatory approaches toward achieving cyber resiliency

In addition to approaches concerned with regulatory compliance, defense contractors might consider leveraging solutions from a nonregulatory standpoint that can be deployed to mitigate the cybersecurity risks.

- **Digitize and automate supply chain functions** – Digitize supply chain functions to bolster access control and traceability (e.g., the use of collaboration and supply chain solutions for high-security and high-compliance environments). Moreover, defense contractors should increasingly automate repetitive analysis workflows using commoditized tools for assessing the cybersecurity profile of subcontractors before accepting them as suppliers. Work to eliminate the reliance on self-reported survey results.
- **Integrate blockchain technology to strengthen security** – Blockchains could help boost cybersecurity as the technology can prevent fraudulent activities through consensus mechanisms and detect data tampering based on its underlying characteristics of immutability, transparency, auditability, data encryption, and operational resilience.
- **Artificial intelligence (AI) and machine learning (ML)** – As adversaries are using new channels and vectors through modern infrastructure attack surfaces, active defense technologies and advanced analytics that incorporate AI and ML can enable organizations to gain broader, real-time visibility into their changing threat landscape and more efficiently detect anomalous activity. With the help of AI and ML, threat detection and incident response time can be significantly reduced. Software that uses AI and ML can provide security threat alerts on a real-time basis. That software, coupled with advanced security automation techniques, can increase the ability to defend cybersecurity attacks in near realtime.

Raytheon, a US-based defense contractor, has invested more than $3.5 billion in cybersecurity initiatives over the last decade. The company expects to further increase investments in cybersecurity-related R&D and acquisitions, as combating cyber threats is becoming a priority for Raytheon and its customers, which includes the US Department of Defense. Since 2007, Raytheon has made 17 cyber-related acquisitions, and it continues to scout for more, according to the chief technology officer of the company's cybersecurity and special missions division.

Source: Raytheon, 2016 10-K report; Raytheon, "Building a cyber powerhouse," August 18, 2015, https://www.raytheon.com/news/feature/cyber_powerhouse, last updated February 5, 2018.

Lockheed Martin, one of the primary weapons suppliers of the world, partnered with Guardtime Federal to integrate blockchain technology into their existing data systems. Their goal is focused on taking steps to prevent the manipulation of their advanced weapons technology and related information.

Source: Lockheed Martin, "Lockheed Martin partners with Guardtime Federal for innovative cyber technology," Press release, July 9, 2018, https://news.lockheedmartin.com/2018-07-09-Lockheed-Martin-Partners-with-Guardtime-Federal-for-Innovative-Cyber-Technology.

Paving the way for cyber resiliency

The initial rollout of DFARS 252.204-7012 and the associated flow-down requirements lacked clarity about how much responsibility prime contractors needed to take in assessing the compliance of their suppliers' cybersecurity controls. However, recent steps taken by the DoD and DCMA to amend the CPSR process clearly show that the DoD expects prime contractors to be proactively and regularly assessing and documenting the adoption of cybersecurity controls by their suppliers.

A foundational step for prime contractors to achieve these objectives is through a supply chain governance program that not only identifies previously unknown and high-risk suppliers but assesses the suppliers' cyber hygiene and continuously monitors their progress toward cyber resiliency and risk mitigation. Success can be influenced by taking a framework approach to identify, prioritize, and address risk and compliance within a prime contractor's ecosystem. Prime contactors' migration toward a robust cyber governance program is critical to help enhance cyber resiliency across the DIB.

Definitions

Ballistic Missile Defense System (BMDS): An integrated, "layered" architecture that provides multiple opportunities to destroy missiles and their warheads before they can reach their targets.[12]

Contractor Purchasing System Review (CPSR): Analyzes how contractors spend government funds, as well as their compliance with government policy when subcontracting.[13]

Covered Contractor Information System (CCIS): An information system that is owned or operated by a contractor that processes, stores, or transmits federal contract information.[14]

Covered Defense Information (CDI): Unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry (http://www.archives.gov/cui/registry/category-list.html), which requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and government-wide policies.[15]

Controlled Unclassified Information (CUI): Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.[16]

Defense Contract Management Agency (DCMA): An agency of the United States federal government reporting to the Under Secretary of Defense for Acquisition and Sustainment (USD). It is responsible for administering contracts for the Department of Defense (DoD) and other authorized federal agencies.[17]

Defense Federal Acquisition Regulation Supplement (DFARS): DFARS to the Federal Acquisition Regulation (FAR) is administered by the Department of Defense (DoD). The DFARS implements and supplements the FAR. The DFARS contains requirements of law, DoD-wide policies, delegations of FAR authorities, deviations from FAR requirements, and policies/procedures that have a significant effect on the public. The DFARS should be read in conjunction with the primary set of rules in the FAR.[18]

DFARS 204.7300: This subpart applies to contracts and subcontracts requiring contractors and subcontractors to safeguard covered defense information that resides in or transits through covered contractor information systems by applying specified network security requirements. It also requires reporting of cyber incidents. This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.[19]

DFARS 252.204-7012: Safeguarding of Unclassified Controlled Technical Information (CTI) clause requires a contractor to report to the DoD the possible exfiltration, manipulation, or other loss or compromise of unclassified CTI; or other activities that allow unauthorized access to a contractor's unclassified information system on which unclassified CTI is resident or transiting. CTI is technical information with military or space application that is subject to controls on its access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.[20]

Defense Industrial Base (DIB): The DoD, US government, and private-sector worldwide industrial complex with capabilities to perform research and development, design, produce, deliver, and maintain military weapon systems, subsystems, components, or parts to meet military requirements. The DIB includes hundreds of thousands of domestic and foreign entities and their subcontractors performing work for DoD and other federal agencies. Defense-related products and services provided by the DIB equip, inform, mobilize, deploy, and sustain forces conducting military operations.[21]

DoD Inspector General (DoDIG): An independent, objective agency that provides oversight related to the programs and operations of the United States DoD.[22]

Missile Defense Agency (MDA): A research, development, and acquisition agency within the US DoD. MDA's mission is to develop, test, and field an integrated, layered, ballistic missile defense system (BMDS) to defend the United States, its deployed forces, allies, and friends against all ranges of enemy ballistic missiles in all phases of flight.[23]

National Defense Industrial Association (NDIA): An educational nonprofit that engages thoughtful and innovative leaders to promote the best policies, practices, products and technology for warfighters and others who ensure the safety and security of our nation. NDIA drives strategic dialogue in national security by identifying key issues and leveraging the knowledge and experience of its military, government, industry, and academic members to address them.[24]

National Institute of Standards and Technology (NIST): A physical sciences laboratory, and a nonregulatory agency of the US Department of Commerce whose mission is to promote innovation and industrial competitiveness. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards and has active programs for encouraging and assisting industry and science to develop and use these standards.[25]

NIST SP 800-171: A codification of the requirements that any nonfederal computer system must follow in order to store, process, or transmit Controlled Unclassified Information (CUI) or provide security protection for such systems. NIST SP 800-171 compliance is currently required by some DoD contracts via DFARS clause 252.204-7012.[26]

Office of the Secretary of Defense (OSD): The principal staff element of the Secretary of Defense in the exercise of policy development, planning, resource management, fiscal, and program evaluation responsibilities. OSD includes the immediate offices of the Secretary and Deputy Secretary of Defense, Under Secretaries of Defense, Director of Defense Research and Engineering, Assistant Secretaries of Defense, General Counsel, Director of Operational Test and Evaluation, Assistants to the Secretary of Defense, Director of Administration and Management, and such other staff offices as the Secretary establishes to assist in carrying out assigned responsibilities.[27]

Plan of Actions and Milestones (POA&M): A key document in the security authorization package and for continuous monitoring activities. The POA&M facilitates a disciplined and structured approach to tracking risk mitigation activities. The POA&M includes security findings for the system from continuous monitoring activities and periodic security assessments such as the Annual Assessment.[28]

System Security Plan (SSP): Main document of a security package in which a cloud service provider (CSP) describes all the security controls in use on the information system and their implementation. Once completed, a SSP provides a detailed narrative of a CSP's security control implementation, a detailed system description including components and services inventory, and detailed depictions of the system's data flows and authorization boundary.[29]

Under Secretary of Defense for Acquisition and Sustainment (USD A&S): A senior civilian official in the Office of the Secretary of Defense (OSD) within the DoD. USD A&S is the principal staff assistant and adviser to the Secretary of Defense and the Deputy Secretary of Defense for all matters concerning the DoD's acquisition and sustainment.[30]

United States Department of Defense (DoD): An executive branch department of the federal government charged with coordinating and supervising all agencies and functions of the government concerned directly with national security and the United States Armed Forces.[31]

Endnotes

1. Symantec, *2019 Internet Security Threat Report*, https://www.symantec.com/en/hk/security-center/threat-report.
2. National Institute of Standards and Technology (NIST), DFARS Cybersecurity Requirements, https://www.nist.gov/mep/cybersecurity-resources-manufacturers/dfars800-171-compliance.
3. Office of the Under Secretary of Defense for Acquisition & Sustainment, Technology and Logistics (USD A&S), 252.204-7012—Safeguarding Covered Defense Information and Cyber Incident Reporting (October 2016), https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012, retrieved April 1, 2019.
4. Joseph Marks, "The Cybersecurity 202: Russia and China hacking with its own influence operations, think tank says," *Washington Post*, February 1, 2019; Lyubov Pronina, "U.S. warns of Russian, Chinese cyber threats at NATO meeting," *Bloomberg*, February 14, 2019, https://www.bloomberg.com/news/articles/2019-02-14/u-s-warns-of-russian-chinese-cyber-threats-at-nato-meeting.
5. NIST, DFARS Cybersecurity Requirements.
6. Office of the USD A&S, Subpart 204.73—Safeguarding Covered Defense Information and Cyber Incident Reporting (Revised December 28, 2017), https://www.acq.osd.mil/dpap/dars/dfars/html/current/204_73.htm.
7. Office of the USD A&S, 252.204-7012—Safeguarding Covered Defense Information and Cyber Incident Reporting (October 2016).
8. Chris Nissen, John Gronager, Robert Metzger, and Harvey Rishikof, *Deliver uncompromised: A strategy for supply chain security and resilience in response to the changing character of war*, The MITRE Corporation, August 2018, https://www.mitre.org/sites/default/files/publications/pr-18-2417-deliver-uncompromised-MITRE-study-8AUG2018.pdf, p. 15.
9. US Department of Defense Inspector General (DoDIG), *Logical and physical access controls at Missile Defense Agency contractor locations*, Report No. DODIG-2018-094, March 29, 2018, https://media.defense.gov/2018/Apr/05/2001899799/-1/-1/1/DODIG-2018-094.PDF.
10. Office of the USD A&S, "Addressing Cybersecurity Oversight as Part of a Contractor's Purchasing System Review," Memorandum from Ellen M. Lord, January 21, 2019, https://www.acq.osd.mil/dpap/pdi/cyber/docs/USA000140-19 TAB A USD(AS) Signed Memo.pdf.
11. Department of Defense, Defense Contract Management Agency, *Contractor Purchasing System Review (CPSR) Guidebook*, February 26, 2019, https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_022619.pdf, p. 100.
12. US DoD, Office of the Secretary of Defense, *2019 Missile defense review*, https://www.defense.gov/Portals/1/Interactive/2018/11-2019-Missile-Defense-Review/The%202019%20MDR_Executive%20Summary.pdf.
13. US DoD, Defense Contract Management Agency (DCMA), *Contractor Purchasing System Review (CPSR) Guidebook*, February 26, 2019, https://www.dcma.mil/Portals/31/Documents/CPSR/CPSR_Guidebook_022619.pdf.
14. Acquisition.gov, Subpart 4.19—Basic Safeguarding of Covered Contractor Information Systems, https://www.acquisition.gov/content/subpart-419-basic-safeguarding-covered-contractor-information-systems.
15. US DoD, Safeguarding Covered Defense Information – The Basics, https://business.defense.gov/Portals/57/Safeguarding Covered Defense Information - The Basics.pdf.
16. National Archives, About Controlled Unclassified Information (CUI), https://www.archives.gov/cui/about.
17. DCMA, About the Agency, https://www.dcma.mil/About-Us/.
18. National Archives, Defense Federal Acquisition Regulation Supplement (DFARS), https://www.federalregister.gov/defense-federal-acquisition-regulation-supplement-dfars-.
19. Office of the USD A&S, Safeguarding Covered Defense Information and Cyber Incident Reporting (Oct 2016).
20. Ibid.
21. US DoD, Under Secretary of Defense for Policy, Assistant Secretary of Defense for Homeland Defense and Global Security – Partnering, https://policy.defense.gov/OUSDP-Offices/ASD-for-Homeland-Defense-Global-Security/Defense-Critical-Infrastructure-Program/Partnering/.
22. US DoD, Office of Inspector General, About DoD Office of Inspector General, https://www.dodig.mil/About/.
23. USA.gov, Missile Defense Agency, https://www.usa.gov/federal-agencies/missile-defense-agency.
24. National Defense Industrial Association, About page, https://www.ndia.org/about.
25. USA.gov, National Institute of Standards and Technology, https://www.usa.gov/federal-agencies/national-institute-of-standards-and-technology.
26. NIST, *Protecting Unclassified Information in Nonfederal Information Systems and Organizations (NIST Special Publication 800-171)*, updated January 14, 2016, withdrawal December 20, 2017, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf.
27. US DoD, Office of the Secretary of Defense, https://dod.defense.gov/About/Office-of-the-Secretary-of-Defense/.
28. Federal Risk and Authorization Management Program (FedRAMP), Developing a Plan of Actions & Milestones (POA&M), https://www.fedramp.gov/developing-a-plan-of-actions-milestones/.
29. FedRAMP, Developing a System Security Plan (SSP), https://www.fedramp.gov/developing-a-system-security-plan/.
30. Office of the USD A&S, Home page, https://www.acq.osd.mil/.
31. USA.gov, US Department of Defense, https://www.usa.gov/federal-agencies/u-s-department-of-defense.

Authors and Contacts

Alan Faver
Partner
Deloitte & Touche LLP
+1 404 220 1701
afaver@deloitte.com

Jeff Lucy
Managing Director
Deloitte & Touche LLP
+1 704 887 1519
jlucy@deloitte.com

Deborah Golden
Principal
Deloitte & Touche LLP
+1 571 882 5106
debgolden@deloitte.com

Aijaz Shaik Hussain
Senior Manager
Deloitte Services LP
+1 615 718 5515
aihussain@deloitte.com

Acknowledgments

The authors would like to thank Robin Lineberger, Mark Burroughs, Siddhant Mehra, and Louverture Jones for their significant contributions to this report. Also, thanks to Jason Brown, Emily Mossburg, Andrew Slaughter, and Lancy Jiang for their help with the development of this report.

Deloitte.