THE AUGUSTA GROUP

FISMA, RMF and DoDI 5000.90

DoD procurement, Supply Chain Risk Management and Cybersecurity

May 2021

Ted Dziekanowski, Andy Watkin-Child, Jason Spezzano, Brian McCarthy

The United States (US) government is aligning its thinking on Supply Chain Risk Management (SCRM). In response, the Department of Defense (DoD) is actively working to develop and deploy cybersecurity and SCRM across the Defense Industry Base (DIB) through Defense Federal Acquisition Regulation (DFARS) and Department of Defense Instructions (DODI). DFARS 252.204.7012 (DFARS 7012) and NIST SP 800.171 required compliance as of December 2017. Making further progress, the DoD released its Interim Final Ruling in November 2020, adding DFARS .7019, .7020, and .7021, requiring contractors and subcontractors within the DIB to be compliant with 800.171 and the implementation of the Cybersecurity Maturity Model Certification (CMMC).

SCRM communications have been on the rise, and the US regulatory requirements regarding Cyber-SCRM continue to develop. The 2020 SolarWinds hack identified issues with Software Supply Chain Security and the continued theft of DoD Intellectual Property. In addition, the COVID pandemic and geopolitical tensions have highlighted persistent risks to US supply chains. This is encouraging the US government to actively manage supply chain risk to protect National Security. The US President signed the Executive Order on America Supply Chains in February 2021[1]. This initiated a 100-day review for supply chain risks across the Federal Government, including defense, public health, IT, communications, power, transportation, and agriculture. The 100-day evaluation assesses the resilience, diversity, and security of supply chains in managing economic prosperity and National Security.

In May 2021, the US President signed an Executive Order (EO) on "Improving the Nations Cyber Security"[2].

"All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order. "[2]

The order set out a range of activities for the Federal Government to assess, make recommendations for, and improve the protection of US National Security. The activities include assessing cybersecurity strategy, cybersecurity implementation, and how to define a response to the cybersecurity challenges the US faces today. The order is focused on making improvements to Federal Systems for the prevention, protection, detection, and remediation from cyber incidents. The EO requires improvements in Federal information sharing, modernization of Federal Government cybersecurity (cloud adoption, zero trust architecture, and FedRamp), oversight and assurance of software supply chain security, enforcement of cybersecurity requirements through acquisition mechanisms, standardization of vulnerability detection, and cyber incident response.

The US Government Accountability Office (GAO) and Office of the DoDs Office of the Inspector General (DoD IG) have highlighted the challenges faced by the DoD in securing Defense weapons systems and Defense IP from Cyber-attack[3-7]. This has raised concerns over the safety and security of DoD weapon systems and affecting their ability to operate within mission-critical environments when faced with Nation-State threat actors.

Cybersecurity and SCRM is a strategic issue for the global DIB and the DoD. The DIB is pivotal in the management of Defense Supply Chain Risk, and the DoD provides the DIB with procurement contracts for the manufacture, service, and support of weapon systems. This process is managed by the DoDs Defense Acquisition System (DAS). The DAS has been implemented to ensure that the DoD is equipped to win military operations against all adversaries in all warfighting domains, including cyberspace. The DAS and associated decision authorities and program managers are the procurement interface between the DIB and DoD. It is the interface where procurement discussions and standards, policies, and procedures are interpreted and applied. The DAS is one mechanism that the DoD uses to remediate the issues identified by the GAO and DoD Inspector General. The DoD has implemented DFARS 7012 (December 2017) and NIST SP 800.171 (NIST) cybersecurity practices for the protection of Controlled Unclassified Information

(CUI). They are in the process of adopting the DoD's CMMC program through the Interim Final Ruling (IFR), which came into force in November 2020.

The Federal Information Security Modernization Act (FISMA) of 2002, and amended in 2014, is an effective regulation mandating reporting requirements. These requirements include implementing standards in the Federal Information Processions Standards (FIPS) and guidelines (NIST) to reduce the security risk to Federal information and data while managing spending on information security. With 8510.01, the DoD adopted FISMA across the Army, Navy, and Air Force[8], mandating policies and procedures based on the NIST SP 800.37, Risk Management Framework (RMF).

DODI 5000.90 - Cybersecurity for acquisition decision authorities and program managers

In December of 2020 the DoD issued DoDI 5000.90 (5000.90) "Cybersecurity for Acquisition Decision Authorities and Program Managers," setting out the foundations for cybersecurity risk-based decision making within the DAS, the RMF, and SCRM policy for program managers. 5000.90 will impact DoD procurement processes, deploying a risk-based cybersecurity oversight and assurance with DAS and impacting the relationship between the DoD and the DIB. 5000.90 establishes policy, assigns responsibilities, and prescribes the procedures for managing cybersecurity risk by program Decision Authorities (DA) and Program Managers (PM) in the DoD acquisition process. 5000.90 requires assessment and management of cyber risk across the acquisition lifecycle. 5000.90 establishes policy, standards, and guidance to qualify and quantify cybersecurity risks across acquisition programs arising from adversaries targeting suppliers and supply chains. This informs investment decisions throughout the procurement lifecycle.

"This policy is necessary to provide consistent guidance for decision authorities and program managers to implement proper levels of cybersecurity processes and practices for every acquisition throughout the supply chain, regardless of which adaptive acquisition framework pathway is used.[10]"

5000.90 sets out four procedures.

Procedure 1. Cybersecurity Foundations in the Defense Acquisition System ("DAS")

The DAS is a core capability in assuring that the DoD is equipped to win military operations in all warfighting domains. It encompassed the DoD's Adaptive Acquisition Framework (Figure 1) applied to the acquisition of weapon systems and processes ranging from service, major capability, urgent capability, software, and business system and R&D acquisition processes. This is for the procurement of platforms, weapon systems, and the DIB, ensuring that cyber risks and cybersecurity are appropriately assessed, resourced, and mitigated within the DoDs supply chain.

"Provides a clear focus on the role of acquisition program managers and decision authorities as coordinators and overseers of all aspects of cybersecurity in acquisition programs. [10]"

Embedding cybersecurity into all aspects of the DAS is critical for securing DoD weapon systems and their DIB. The DAS enables procurement DAs and PMs to reinforce cybersecurity through the deployment and continual reinforcement of cybersecurity risk management practices. They are making risk-based procurement decisions through existing procurement processes, with the potential of refusing to award the DIB contracts based on the adoption of poor cyber risk management e.g. CMMC[11].

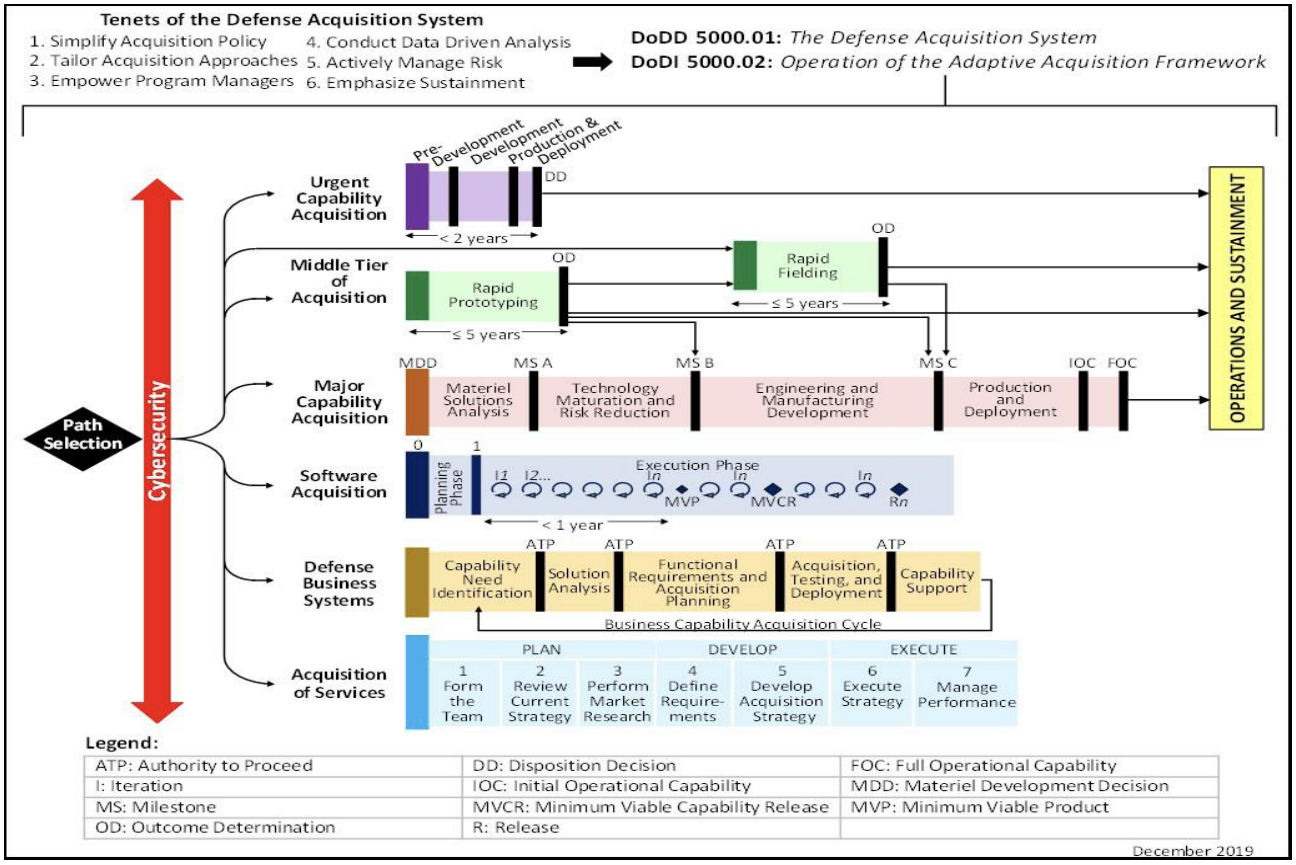

Figure 1. The Adaptive Acquisition Framework (AAF)

Procedure 2. Cybersecurity Driven by Threat

5000.90 sets out the responsibilities of DoD procurement DAs and PMs to incorporate cybersecurity requirements and apply controls to mitigate anticipated emerging threats. This is so that DoD systems are effective in their operational environments. The DoDI requires program managers as part of the RMF and NIST SP 800.37r2 to:

(1) Perform system threat analysis, using information produced by the Intelligence community, in the development of cybersecurity strategy and assessment of risk.
(2) Link threat mitigation with the Authorization to Operate (ATO).
(3) Continually review cyber threats throughout the acquisition lifecycle, initiate risk assessment as and when new cyber threats are identified, and conduct an appropriate operational risk assessment, identifying the risk to the enterprise and mission.
(4) Tailor the RMF process to achieve an Authorization to Operate (ATO) commensurate with the program's cyber risk.

Procedure 3. Cybersecurity Planning and Execution

a. Planning cybersecurity activities

DoDI 5000.02T, "Operation of the Defense Acquisition System," articulates the role of the PM to produce a Cyber Security Strategy. Detailing how the procured system will operate in a cyber-contested environment and where an ATO is required, documenting:

(1) A Plan of Action and miles stones (POA&M) is included to address known vulnerabilities.
(2) Continuous monitoring of risks based upon cyber threats, vulnerabilities, and mitigations.
(3) Implement the Risk Management Process (RMF) within the PMs office's acquisition, engineering processes for development, procurement, testing, and sustainment.

(4) The need for operational cyber resilience and, if appropriate, the resulting monitoring, responding, and recovering of the system and mitigation of the vulnerabilities.

b. Executing Cybersecurity Throughout the Acquisition Lifecycle

DoDI 5000.85 "Major Capability Acquisition", 3C.3 defines the responsibilities of the PM for the development, production, deployment, sustainment, and supportability of new defense systems. Management activities are designed to achieve the cost, schedule, and performance of the program. This ensures that cybersecurity risks are assessed and managed throughout the acquisition lifecycle. To meet these requirements:

(1) PM's will allocate resources and personnel to mitigate cyber risk.
(2) PMs should conduct periodic threat-representative adversarial assessments to assess the ability of the cyber technologies in the materiel solution to complete missions in a cyber- contested environment.
(3) If an ATO is required, identify the AO responsible and ensure they are informed on cyber risks, threats, and associated mitigations for the program to operate in a threat-informed, cyber-contested environment.
(4) Implement threat-based cybersecurity throughout the Acquisition Lifecycle (Figure 2), detailing how PMs will design, build, test, field, and sustain their product. Likewise, PMs have associated cybersecurity activities they must accomplish and must define their cybersecurity strategy, which continues through the RMF process leading to an ATO.
(5) PMs, in coordination with AOs, must revisit a program's cybersecurity posture based on threat assessments and continuous monitoring.
   a. While the AO may authorize a continuous ATO (cATO), a cATO is only appropriate for products that have a robust automated monitoring capability that allows real or close to real time situational awareness of their cybersecurity status.
   b. The iterative ATO process depicted in Figure 2 enables AOs to monitor risks codified in security assessment reports and progress against the program's cybersecurity strategy and cybersecurity POA&Ms, all based on threat assessments from the Intelligence Community.

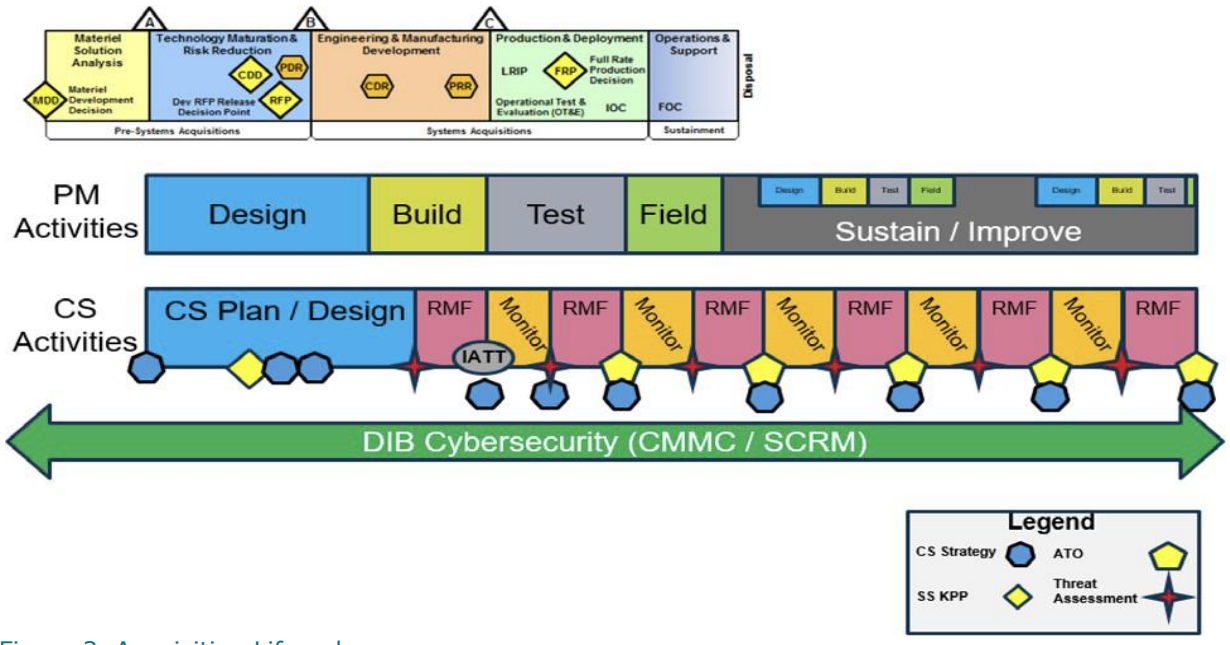

Figure 2. Acquisition Lifecycle

c. Resourcing Cybersecurity Activities

The PM is responsible for ensuring that adequate resources are allocated to oversight and assurance. In addition to allocating and protecting resources to constantly improve software, manufacturing, and reliability throughout a program's lifecycle, dedicating program resources and personnel to continually assess and mitigate the program's cybersecurity risk by monitoring:

(1) New techniques and technologies for potential inclusion in the system baseline to improve it's abilities to protect, detect, and recover from attacks.
(2) The emergence of exploitable cyber vulnerabilities.
(3) Methods to eliminate or mitigate vulnerabilities in accordance with DoD CIO guidance regarding vulnerability management.
(4) The threat environments where the system is, or is to be, deployed to determine if there are major changes that require updates to the system's cybersecurity controls.

Procedure 4. – Cybersecurity in the Supply Chain

DoD weapon systems rely upon national and international supply chains for their procurement, manufacture, service, and support, including IP from the DoD to Prime defense contractors and subcontractors. US strategic competitors have been exploiting and stealing IP from the DIB, decreasing confidence in the security of products delivered to the DoD. Contractor facilities, including design, development, and production environments, networks, supply chains, and personnel, are being used by threat actors as cyber pathways to access government programs. This includes government organizations and fielded systems to steal, alter, or destroy system functionality, information, or technology.

The DAS and the DIB play a pivotal role in securing the DoDs IP across the supply chain. PMs are essential components in SCRM performing the following tasks.

(1) They will conduct SCRM, including Cyber-SCRM. At a minimum, conducting market research to assess potential vendors to determine if they:
   a. Provide products and components, or sub-components, sourced through original equipment manufacturers or authorized resellers.
   b. Have previously incurred significant malicious network intrusions, data breaches, loss of client data, or intellectual property.
   c. Have obtained a CMMC certification level indicating that they practice, at least, basic cyber hygiene (e.g., access management, timely patch management, identity management, and password management).
(2) PMs will consider maintaining a visualization (illumination) of the supply chain to have situational awareness of the risks and vulnerabilities throughout the program's supply chain, especially those on the USD(R&E) Critical Technology List.
(3) PMs will:
   a. Consider the source of products that may be supplied to fulfill program requirements and seek alternatives to design of performance specifications or other program requirements that may necessitate the use of sources owned by, controlled by, or subject to the jurisdiction of a foreign adversary's government. The program PM will maintain a complete list that shows to the furthest extent possible:
   b. The ownership of commercial companies that currently do, or potentially will, supply (hardware, software, or firmware) components to the program, and therefore may be subject to influence or control by threat actors with a known interest in the IS or PIT being acquired by the program.
   c. Technology relationships with other companies that are known to already be under the influence or control of threat actors.
   d. Take action to manage supply chain risks, including those associated with foreign ownership, control, or influence concerns, commensurate with the risk tolerance level of the system or mission in question.

e. Counter risks to and from a product by applying a framework for cybersecurity SCRM due diligence that links supply chain risk tolerance with the importance of the systems purchased.

High Risk Tolerance	High risk tolerance applies to simplified procurements, like computers at the Defense Commissary Agency. PMs should: • Exercise caution regarding products originating from sources with identified foreign ownership, control, or influence concerns. • Utilize approved products lists. • Maintain assurance through industry standards. • Balance risk against mission type.
Moderate Risk Tolerance	Moderate risk tolerance applies to structured procurements, like wireless networks at a forward deployed base. PMs should implement all previous strategies and: - Use verifiable vendor processes for product integrity (e.g., SSAE18-SOC2). - Improve awareness of vendor/product limitations. - Manage critical SCRM risks through countermeasures.
Low Risk Tolerance	Low risk tolerance applies to engineered procurements, like industrial control systems in a tank. PMs should implement all previous strategies and: - Assess critical components. - Implement available countermeasures. - Utilize commercial assessment vendors, the Joint Federated Assurance Centre, interagency and close and trusted international partners, national labs/FFRDCs, and intelligence and CI.
Very Low Risk Tolerance	Very low risk tolerance applies to assured procurements, like nuclear command and control systems. PMs should implement all previous strategies and: - Follow all requirements in DoDI 5200.44 and NIST SP 800-161; including: • Conducting criticality analysis. • Documenting in Program Protection Plan. • Sending requests on critical components/suppliers to the DIA SCRM TACor other CI sources. • Flagging reports that come back critical, high, or select medium. Utilize the scoping and mitigations process to make mitigation decisions commensurate with risk.

Table 1. SCRM Actions by Risk Tolerance

(4) Use assured suppliers or appropriate SCRM countermeasures for system elements that perform mission-critical functions. In accordance with DoDI 5200.44, cyber protection measures for mission-critical functions and critical components must, at minimum, include the following:
a. Software assurance.
b. Hardware assurance.
c. Procurement strategies.
d. Anti-counterfeit practices.

Conclusion

The DoD is undergoing a significant transformation to achieve superiority against all adversaries in all warfighting domains, including cyberspace. Therefore, risk management, SCRM, and cybersecurity has been developing across the Federal Government since the passing of the FISMA in 2002 and its update in 2014, with the DoD formalizing the RMF across the Army, Navy, and Air Force, requiring the services to adopt a risk-based approach to weapon system acquisition.

In the authors' opinions, DoDI 5000.90 is the first acquisition document representing a bridging of FISMA, RMF, SCRM, and cybersecurity requirements setting out the risk management practices, oversight, and assurance requirements for cyber risk between the DoD to the DIB. 5000.90 provides consistent guidance for DAs and PMs to oversee cybersecurity, risk management processes and practices for every defense acquisition throughout the supply chain.

5000.90 sets out a risk-based classification structure for cybersecurity through risk tolerance levels. The approach should benefit both the DoD and the DIB to manage cybersecurity and improve oversight and assurance based upon risk prioritization. Lower risk systems require fewer controls, less oversight, and assurance when compared to high-risk (low-risk tolerance) ones (Table 1 above). Given the existing constraints on resources, the complexity of multi-national agreements, and the impact on innovation, adopting the risk-based model put forth in 5000.90 represents an opportunity for prioritizing risk mitigation on critical systems. Furthermore, alternative mechanisms such as SOC2 Audits to assure cyber compliance could be considered to reduce the impact on the majority of suppliers in the DIB (Table 1. SCRM Actions by Risk Tolerance - Moderate).

References

1. SCRM Executive Order, February 24, 2021: https://www.federalregister.gov/documents/2021/03/01/2021-04280/americas-supply-chains
2. Cybersecurity Executive order, May 2021: https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/
3. Government Accountability Office (2018): Weapon Systems Cybersecurity: DOD Just Beginning to Grapple with Scale of Vulnerabilities
4. Government Accountability Office (2018): Urgent Actions Are Needed to Address Cybersecurity Challenges Facing the Nation
5. Government Accountability Office (2018): DOD Just Beginning to Grapple with Scale of Vulnerabilities
6. Government Accountability Office (2021): WEAPON SYSTEMS CYBERSECURITY Guidance Would Help DOD Programs Better Communicate Requirements to Contractors
7. Government Accountability Office (2021): Drive to Deliver Capabilities Faster Increases Importance of Program Knowledge and Consistent Data for Oversight
8. Office of the Inspector general US DoD (2019): Audit of Protection of DoD Controlled Unclassified Information on Contractor-Owned Networks and Systems DODIG-2019-105
9. US Airforce RMF Framework (2020): https://static.e-publishing.af.mil/production/1/saf_cn/publication/afi17-101/afi17-101.pdf
10. OUSD A&S - DOD 5000 Series Acquisition Policy Transformation Handbook https://www.acq.osd.mil/ae/assets/docs/DoD%205000%20Series%20Handbook%20(09%20FEB%2021).pdf
11. CMMC and NIST: Interim Final rule - D041