ICRMAT 2022
Proceedings of the International Conference on Research in Management & Technovation pp. 37–41
DOI: 10.15439/2022M8894
ISSN 2300-5963 ACSIS, Vol. 34

Integration of Supply Chain Risk Management into the Enterprise Risk Management Program for the Department of Defense

S. Raschid Muller, Ph.D., MBA
Assistant Professor of Cybersecurity
Capitol Technology University
Laurel, MD, USA
Email: srmuller@captechu.edu
https://orcid.org/0000-0002-1742-7575

Corey E. Thomas, LTC, US Army
Administrative Law Attorney
National Guard Bureau
Washington, DC, USA
Email: cethomas1091@gmail.com

***Abstract*—This paper explores supply chain risk management (SCRM) integration into the enterprise risk management (ERM) program across the Department of Defense for three main reasons: responsibility, necessity, and visibility. Multiple laws, orders, policies, strategies, and standards hold Federal leaders responsible for their agencies' performance. The current global nature of the DoD's supply chain, its dependency on information technology, and the constant threats in the cyber realm make it necessary to integrate SCRM into the ERM program. Should DoD leadership lose sight of these threats, the impact on the enterprise could be catastrophic. As a result, DoD leaders must maintain the visibility of the supply chain as part of the ERM program. While many organizations have treated SCRM and ERM separately throughout the years, technology and the exponential growth of cyber threats have brought those days to a close. The importance of the supply chain to mission accomplishment, coupled with persistent threats in the cyber-realm, dictates the integration of SCRM and ERM as a requirement. This paper explains the issues above while giving multiple examples of why integration is imperative. Should the DoD make SCRM part of its ERM program, the chances of remaining a dominant global force will continue well into the future for Cybersecurity professionals working in U.S. organizations.**

***Index Terms*—cybersecurity, supply chain risk management, DoD, policy, enterprise risk management.**

I. Introduction

The Department of Defense (DoD) should integrate supply chain risk management (SCRM) into its enterprise risk management (ERM) program for three main reasons: responsibility, necessity, and visibility. Before analyzing these three prongs, it is necessary to gain a clear understanding of ERM and SCRM. This understanding makes the importance of integrating SCRM into the DoD's ERM program more apparent.

II. Literature Review

Enterprise Risk Management is a methodology used to identify, address, and control risks that affect the entire organization [1]. Instead of individually addressing risks based on organizational function or activity, ERM addresses interdependence and sheds light on the second and third-order effects across the enterprise should an incident occur in one of its functions, like the supply chain [1]. Figure 1 below is a depiction of the main elements of the ERM process. When starting the process, organizational leaders should consider various factors such as laws and policies, foreign relationships, resources, etc. [1]. The next step, the identification of risks [2], is critical because, in the supply chain, the risk is not merely the prime contractor. Still, it may likely be the prime contractor's subcontractors and all of their suppliers. Therefore, leadership must clearly define and scope the problem. The issue here is if the risks and threats faced by functions like the supply chain are discussed in silos instead of upfront as part of the ERM program, then organizational leadership will always be in a reactive mode, addressing the problems after the damage.

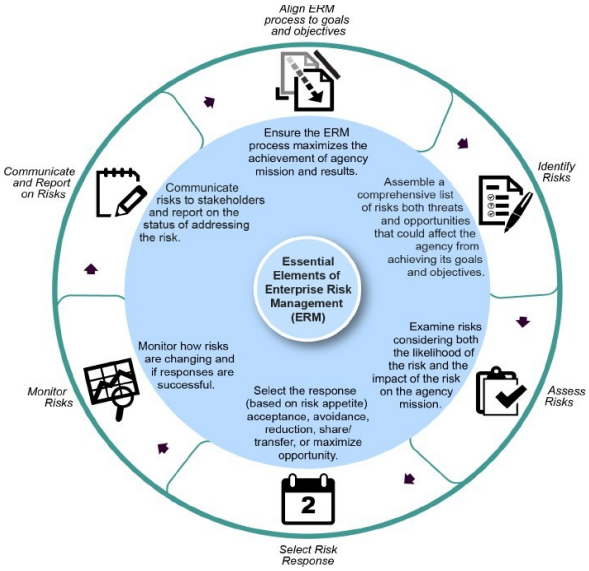


Figure 1. A graphic depicting the critical elements of enterprise risk management as provided by GAO for use by the Federal government. Retrieved from Enterprise Risk management: Selected Agencies' Experiences Illustrate Good Practices in Managing Risk, by the U.S. Government Accountability Office, December 2016, GAO-17-63, p. 8.

Understanding ERM enables an easier understanding of SCRM. One need only replace the word "enterprise" with "supply chain." While there are issues unique to the supply chain, the methodology and theory are the same. The supply chain is an integral part of the enterprise. To be clear, an enterprise cannot function properly without its supply chain. For the DoD in the continental United States (CONUS) or beyond, the enterprise relies heavily on its supply chain to deliver mission-critical goods and services. From the provision of information technology (IT) experts to support the day-to-day mission in the National Capital Region (NCR) and abroad, or delivery of equipment, weapons, material, or information and communications technology (ICT), the DoD supply chain is essential to mission accomplishment.

However, risk comes along with having a supply chain. Historically, leaders assessed supply chain risk as a function of cost, schedule, and performance (National Counterintelligence and Security Council, n.d.). As demonstrated by Figure 2 below, because of today's global environment populated that is constantly experiencing technological change joined by a growing population of harmful cyber-threats, a fourth element must be added to the equation, security. These risks, coupled with other factors such as organizational interdependencies, U.S. and international laws, policies, etc., must be considered when conducting SCRM.

Figure 2. A graphic depicting the equation used to express supply chain risk in the cyber-realm. Retrieved from Supply Chain Management: A Framework for Assessing risk, by the National Counterintelligence and Security Center, n.d., p. 1.

III. Responsibility

The agency head is responsible for its performance. However, there are tools in place to help provide guidance. These tools come from federal laws, executive orders, presidential directives, DoD policies, and industry standards. Many of these artifacts require the agency head to engage in ERM. With that said, the DoD cannot adequately perform ERM without managing supply chain risk as part of the program. Arguably, the same holds for all other Federal government departments and agencies.

The Federal Managers' Financial Integrity Act (FMFIA) of 1982 requires all Federal managers to control their agency and its assets effectively. The supply chain is how DoD agencies receive and manage their assets. Therefore, agency heads cannot fulfill their responsibilities under the Act without considering how supply chain risks may affect the enterprise. Under the authority of the FMFIA, Office of Management and Budget (OMB) Circular A-123, first published in 1981, was issued to all elements of the DoD to strengthen internal controls [3]. According to a 2016 memorandum submitted by OMB's director to the heads of all Executive departments and agencies, ERM is an essential control function and must be appropriately conducted [3]. The proper conduct of ERM includes the assessment of all risks to the enterprise, including the supply chain. A 2019 survey issued to organizational leaders throughout the Federal government revealed that cybersecurity and compliance with OMB Circular A-123 were top concerns for all respondents [4]. Even though the survey also found that most of the respondents had an ERM program, there was no indication that SCRM was integrated into their ERM programs [4].

Four years after the issuance of OMB Circular A-123, OMB Circular A-130 was published. As revised in 2000, this circular directs agencies to manage information as a strategic resource [5]. The policy includes the security of information technology (IT) [5]. Information technology is used throughout the DoD supply chain. From how the DoD qualifies suppliers and acquires goods and services to manufacturing processes and system delivery, the DoD supply chain relies heavily on IT. This reliance is why IS throughout the supply chain is so important as an element of SCRM and serves as yet another reason why integration into the DoD ERM program is required.

After OMB Circulars A-123 and A-130, the Federal Acquisition Supply Chain Act (FASCA) of 2018, Title II of 2018 Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure (SECURE) Technology Act was passed. To help strengthen security within the Federal supply chain, FASCA 2018 modified Title 41 of the United States Code (public contracts). This modification caused Federal leaders, including those within the DoD, to take a more critical look into their supply chains, especially when dealing with IT procurement [6]. The requirement for a more in-depth look into supply chain risk represents a good reason to integrate SCRM into ERM. The DoD does not have to sacrifice supply chain security to maintain global competitiveness, nor do regulations and oversight have to burden operations.

In most cases, like the FASCA, rules are in place to help to ensure continued operations. In this case, the rules require DoD leaders to manage supply chain risk while accomplishing the mission. Accordingly, here is yet another reason Federal laws and policies require that the DoD ensure the security of its supply chain and any IT procured through it. Because IT is heavily used throughout the DoD supply chain, SCRM should be incorporated into the DoD ERM program.

Even the Executive Office has weighed in on supply chain security and its effect on the DoD enterprise. In 2009, the White House released The Comprehensive National Cybersecurity Initiative. In the initiative, President Obama directed the Executive Branch to work with all key players, including State and local governments, to promote the unity of effort when responding to future cyber-attacks [7]. The notice contains twelve specific initiatives. The eleventh initiative requires leadership to develop and incorporate a program to manage supply chain risk across the enterprise [7]. The President followed up in 2012 by issuing the National Strategy for Global Supply Chain Security. While a global supply chain reduces trade barriers and bolsters the American economy, security must be in place to protect the supply chain from internal and external threats [8]. Therefore, it stands to reason that to help ensure a more operable, secure, and resilient supply chain; DoD leaders should incorporate SCRM into their ERM program. To do otherwise would place too much distance between the DoD leadership and supply chain cyber threats that could bring organizational operations to a screeching halt.

To align with the Federal rules, the DoD has issued multiple policies. For instance, Department of Defense Instruction (DoDI) 4140.01, DoD Supply Chain Material Management, provides direction on how the DoD addresses the supply chain's cybersecurity risks, including subcontractor qualification requirements and software procurement [9] (2019). While DoDI 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks, sets the standard for SCRM across the DoD and briefly mentions ERM, it does not draw the connection between the two

(2012). However, DoDI 5000.02, Operation of the Defense Acquisition System, makes it clear that "[a] supply chain is at risk when an adversary may sabotage, maliciously introduce an unwanted function, or otherwise subvert the design, integrity, manufacturing, production, distribution, installation, operation, or maintenance of a system …" (p. 167). If second and third-tier suppliers are not checked, if the origins of parts or algorithms are not closely scrutinized, the door will be open for bad actors to find their way into DoD through the supply chain. Unlike a kinetic attack that may disrupt operations in a specific location, cyber-attacks have no boundaries. It necessarily follows, therefore, that because of the interdependency between DoD IT systems, the effect of a cyber-attack on one DoD agency's supply chain would not stop at the agency. Instead, the potential damage would likely spread enterprise-wide if not quickly detected and responded to following the risk management framework for supply chains [10] . This scenario is another reason SCRM should be incorporated into the DoD ERM program. Yes, SCRM is an excellent way to mitigate cybersecurity risks to the supply chain. However, as explained in volume 1 of DoD Manual (DoDM) 4140.01, a disrupted supply chain, regardless of DoD agency, poses critical risks to the DoD enterprise [11]. Thus, supply chain risk cannot be viewed in a bubble. Instead, the risk to the DoD supply chain must be incorporated into its ERM program.

IV. Necessity

Even if there were no Federal laws and policies governing supply chain management and information security, the cyber risks facing the DoD supply chain make it necessary to incorporate SCRM into the DoD ERM program. Such integration would equip leaders with the timely, relevant information necessary to make critical decisions for the enterprise. In a 2013 article in the American Journal of Industrial and Business Management, several authors joined to drive home the necessity of integrating SCRM into ERM [12]. The authors posit that not only can SCRM provide organizations with an advantage over others, but that advantage can be enhanced if SCRM is made part of ERM [12]. The authors suggest that ISO 31000 can serve as the guideline for integration [12].

In its special publication (SP) 800-161, the National Institute of Standards and Technology (NIST) suggests four elements of SCRM. As Figure 3 below depicts, security is one of those four elements. Information transmission and storage security become more significant as the DoD supply chain continues to increase reliance on IT. When the NIST speaks of information security, the concern is the information's confidentiality, integrity, and availability [10]. Theft of the information is a concern for the DoD. Concurrently consider exploiting any of the SCRM elements, security, for example [10]. If bad actors could gain access to a DoD system and exercise any form of control, significant harm could result, ranging from loss of information to loss of life. Further, issues such as infected IT products and weak suppliers within the DoD supply chain can grant bad actors access to the DoD information network (DoDIN). Such critical threats make it necessary to integrate SCRM into the DoD ERM program.

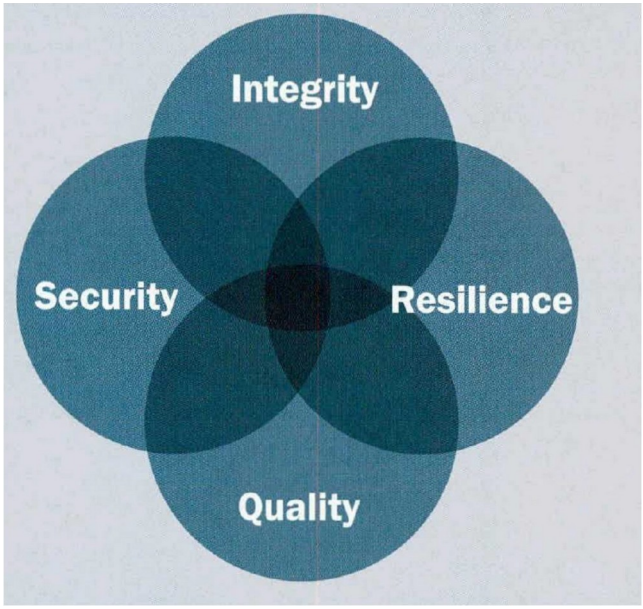


Figure 3. A depiction of the four pillars of information and communications technology (ICT) SCRM as posed by the NIST. Retrieved from, Supply Chain Risk Management Practices for Federal Information Systems and Organizations, by J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, NIST SP 800-161, April 2015, p. 4.

In 2018, the GAO published a report highlighting the supply chain risks affecting Federal agencies related to procuring information and communications technology (ICT). Because of the nature of ICT, bad actors can infiltrate poorly managed global supply chains by introducing malware or malicious algorithms. At a minimum, the Act would disrupt the supply chain, and the worst-case scenario, supply chain failure across the enterprise resulting in mission failure and loss of life [14].

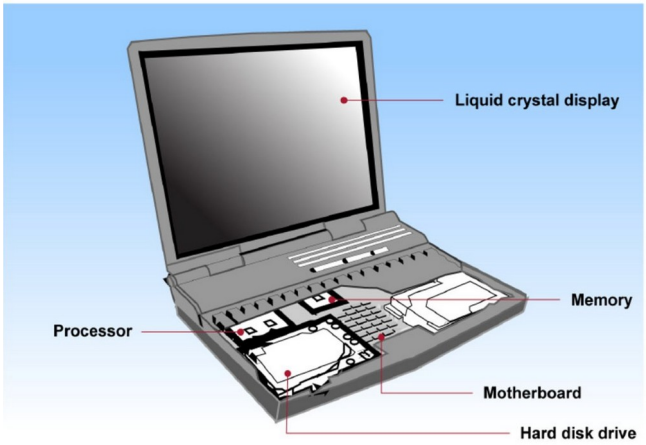
To further illustrate the threat communicated by GAO, consider the 2010 Defense Industrial Base (DIB) Sector-Specific Plan (SSP) published by the Department of Homeland Security (DHS). The DHS designated the DoD as the sector-specific agency (SSA) for the Defense Industrial Base Sector [15]. In the DIB sector-specific plan, the DoD articulates the value of its partnerships with hundreds of thousands of organizations in the private sector [15]. Each one of the partner organizations has relationships with multiple other entities that provide them with IT and various other products that ultimately reach DoD information systems or equipment. Thus, supply chain corruption may not only affect a local DoD system, but it could also cause a ripple of system failures across the enterprise. For example, the DoD procures thousands of laptops for use on DoDIN. As Figure 4 demonstrates, many of the items used to make these laptops could come from suppliers in multiple foreign countries. The systems used by the laptop parts suppliers may be open to hackers. As a result, once their parts are passed through to the DoD, so is the threat.

However, bad actor access does not have to be as intricate as corrupting parts used to manufacture a laptop. For example, certain DoD personnel can procure IT products with government purchase cards. Cimpanu reported how hackers infiltrated certain wireless USB dongles to access organizations' information systems [11]. Many of these wireless

USB dongles were inserted into mice used with DoD laptops. Even though this issue was identified in 2016, and because these supply chain risks are not addressed as part of the ERM program, DoD agencies have continued to allow individuals to purchase and distribute these vulnerable mice. Hence, vulnerable equipment such as laptops and mice represent ways bad actors may access the DoD information network (DoDIN). For DoD leadership to effectively mitigate these risks, it is necessary to incorporate SCRM into the ERM program.

V. Visibility

The final reason the DoD should integrate SCRM into its ERM program is supply chain visibility. To minimize risk to the enterprise, leaders must maintain consistent visibility of their supply chain, especially when the procurement of ICT is involved. As Figure 5 below illustrates, the further away supply chain operations get away from organizational leadership, the less visibility top leadership has, and the higher the risk to the enterprise. This model does not mean that top DoD leaders should know everything about the qualification process for each of the hundreds of thousands of first, second, and third-tier suppliers of each agency. Such an effort is unrealistic, time-consuming, and likely impossible. Figure 5 also demonstrates how visibility is reduced and risk increases as one moves further down the supply chain. With that said, if only one hacker infiltrates one sub-tier supplier, that could be enough to cause critical damage across the DoD enterprise. As a result, DoD leaders should include SCRM as they consider and manage risk to the enterprise.



Component	Location of facilities potentially used by suppliers
Liquid crystal display	China, Czech Republic, Japan, Poland, Singapore, Slovak Republic, South Korea, Taiwan
Memory	China, Israel, Italy, Japan, Malaysia, Philippines, Puerto Rico, Singapore, South Korea, Taiwan, United States
Processor	Canada, China, Costa Rica, Ireland, Israel, Malaysia, Singapore, United States, Vietnam
Motherboard	Taiwan
Hard disk drive	China, Ireland, Japan, Malaysia, Philippines, Singapore, Thailand, United States

Figure 4. A picture showing how the various parts used to create a laptop may be procured from multiple foreign countries. Retrieved from Supply Chain Risks Affecting Federal Agencies, by the U.S. Government Accountability Office, July 12, 2018, GAO-18-667T, p. 4.

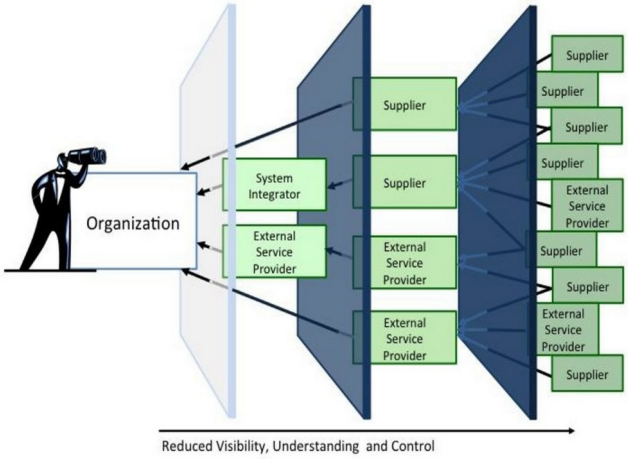


Figure 5. A depiction of how top leadership's visibility decreases the further one moves down the IT supply chain. Retrieved from Supply Chain Risk Management Practices for Federal Information Systems and Organizations, by J. Boyens, C. Paulsen, R. Moorthy, and N. Bartol, NIST SP 800-161, April 2015, p. 8.

To further illustrate the point made by NIST in Figure 5, the NCSC has demonstrated how security, one of the elements of supply chain risk, introduces additional, far-reaching risks to the enterprise (NCSC, n.d.). As demonstrated by the NCSC in Figure 6, to properly understand the security risk facing a supply chain, leadership must understand the "threat, vulnerabilities, and consequences" (NCSC, n.d., para. 3). When considering the threat, leadership should ask questions like, what does the bad actor want (NCSC, n.d., para. 3)? Vulnerabilities in supply chains procuring ICT are both internal and external (NSCS, n.d.). The question is whether a bad actor can reach the DoD through those vulnerabilities within the supply chain (NSCS, n.d.). Consequences range from those that can be addressed and recovered to those that will cripple the enterprise (NSCS, n.d.). DoD leadership must consider these risks throughout the lifecycle of any system it procures, concept through retirement (NSCS, n.d.). Typically, DoD leadership reviews procurement and fielding plans for any major system. However, recent events have shown that, because of the potential impact that an IT security breach may have on the enterprise, more attention should be paid to the procurement of smaller IT-enabled items like laptops and wireless mice. Therefore, it makes even more sense for leadership to integrate SCRM as part of the ERM program for visibility purposes.

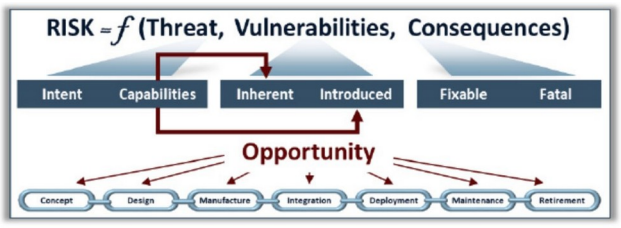


Figure 6. A depiction of threats and vulnerabilities can impact the organization throughout the supply chain by using the system lifecycle concept as an example. Retrieved from Supply Chain Management: A Framework for Assessing risk, by the National Counterintelligence and Security Center, n.d., p. 2.

VI. Conclusion

To satisfy responsibility, necessity, and visibility, it only makes sense for the DoD to include SCRM within its ERM program. Federal laws and policies make it clear that DoD leaders are responsible for the overall health of their supply chains, which includes information security. The forever changing and increasing threats to the DoD's IT-dependent supply chain make SCRM and ERM integration necessary. Because of these threats, DoD leadership must maintain visibility of the risks facing their supply chains. The results of the alternative are grave. On the whole, integration of SCRM into its ERM program will allow the DoD to remain a dominant power across the globe for years to come.

Figures

- **Figure 1.** A graphic depicting the critical elements of enterprise risk management as provided by GAO for use by the Federal government. Retrieved from: https://www.gao.gov/assets/690/681342.pdf
- **Figure 2.** A graphic depicting the equation used to express supply chain risk in the cyber-realm. Retrieved from: https://www.dni.gov/files/NCSC/documents/supplychain/20190422-SCRM-Framework-for-Assessing-Risk.pdf
- **Figure 3.** A depiction of the four pillars of information and communications technology (ICT) SCRM as posed by the NIST. Retrieved from; https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
- **Figure 4.** A picture showing how the various parts used to create a laptop may be procured from multiple foreign countries. Retrieved from: https://www.gao.gov/assets/700/693064.pdf
- **Figure 5.** A depiction of how top leadership's visibility decreases the further one moves down the IT supply chain. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161.pdf
- **Figure 6.** A depiction of threats and vulnerabilities can impact the organization throughout the supply chain by using the system lifecycle concept as an example. The National Counterintelligence and Security Center adapted this picture from the Defense Science Board Task Force Report, Resilient Military Systems, and the Advanced Cyber Threat. Retrieved from: https://nsarchive2.gwu.edu/NSAEBB/NSAEBB424/docs/Cyber-081.pdf

References

[1] U.S. Chief Financial Officers Council (USCFOC), Playbook: enterprise risk management for the U.S. federal government, 2016

[2] U.S. Government Accountability Office (GAO), Enterprise risk management: selected agencies' experiences illustrate practices in managing risk, 17-63. (2016).

[3] Donovan, S., OMB circular no. A-123: management's responsibility for enterprise risk management and internal control, 2016

[4] Association for Federal Enterprise Risk Management (AFERM), Federal enterprise risk management survey results, (2019).

[5] Office of Management and Budget (OMB). Circular no. A-130: Management of federal information resources. 2000.

[6] Federal Acquisition Supply Chain Act (FASCA) of 2018, Title II of the SECURE Technology Act (Strengthening and Enhancing Cybercapabilities by Utilizing Risk Exposure) (H.R. 7327, 41 USC Chap. 13 Subchap. III and Chap. 47, P.L. 115-390)

[7] Obama, B. The comprehensive national cybersecurity initiative, 2009.

[8] Obama, B. National strategy for global supply chain security, 2012.

[9] Department of Defense Instruction (DoDI) 4140.01. DoD Supply Chain Material Management , 2019.

[10] Boyens, J., Paulsen, C., Moorthy, R., & Bartol, N., Supply chain risk management practices for federal information systems and organizations. National Institute of Standards and Technology (NIST) Special Publication (SP) 800-161. 2015

[11] Cimpanu, C., Logitech wireless USB dongles vulnerable to new hijacking flaws, 2019

[12] Scannel, T., Curkovic, S., & Wagner, B. Integration of ISO 31000:2009 and supply chain risk management. American Journal of Industrial and Business Management, 3, 367-77., 2013.

[13] Department of Defense Manual (DoDM) 4140.01, vol.1. DoD Supply Chain Material Management Procedures: Operational Requirements.

[14] U.S. Government Accountability Office (GAO) 18- 667T, Information security: supply chain, 2018.

[15] Department of Defense Instruction (DoDI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Sysxtems and Networks., 2018

[16] U. S. Department of Defense, Defense Science Board (DoDDSB), Task force report: resilient military systems and the advance cyber threat, 2013.

[17] Department of Defense Instruction (DoDI) 5000.02, Operation of the Defense Acquisition System, (2019).

Dr. S. Raschid Muller is a Senior Cybersecurity SME with the Department of Defense (DoD) at Fort Meade, Maryland. He teaches cybersecurity at the undergraduate and graduate levels at Arizona State University, the University of Maryland Global Campus, and Capitol Technology University. Dr. Muller is a 2020 Brookings Institute Fellow (LEGIS) who served on the House Committee for Homeland Security and was assigned to the Cybersecurity, Infrastructure Protection, and Innovation subcommittee in the United States Congress. He also is a 2021 U.C. Berkeley Executive Leadership Academy Fellow from the Goldman School of Public Policy. He is a member of IEEE, ISACA, NDIA, and AFCEA.

LTC Corey E. Thomas, Esq. is a Senior Administrative Law Attorney in the United States Army Judge Advocate General Corps. He graduated from Morehouse College, the University of Arkansas-Little Rock Bowen School of Law, The General Staff and Command College, and the National Defense University. Before joining the National Guard Bureau, he served as the Director for Domestic Operations at The Center for Law and Military Operations (TJAGLCS) in Charlottesville, Virginia. He is admitted to practice law in Arkansas state courts, the federal Eastern and Western Districts of Arkansas, the United States Court of Appeals for the Armed Forces, and the United States Supreme Court.