Enhancing Cybersecurity Through a Revised Risk Management Framework

Juan Paula Jr. and Timothy Shives
Naval Postgraduate School[1], Monterey, USA

Juan.Paula@nps.edu
Timothy.Shives@nps.edu

Abstract: The Department of Defense (DoD) relies on a secure and resilient communication infrastructure to enable critical functions and command and control operations. Ensuring the security of this infrastructure is essential, and the DoD follows the Risk Management Framework (RMF) established by the National Institute of Standards and Technology (NIST) to assess and manage cybersecurity risks. While the RMF is designed to standardize security practices across the DoD, the current process suffers from several shortcomings. These include excessive subjectivity, inefficiencies, and a compliance-driven focus that does not adequately address the rapidly evolving technological landscape and emerging threats. This paper seeks to explore revisions to the RMF that could improve its objectivity, efficiency, and threat-based focus, ultimately enhancing its overall effectiveness. By reviewing existing literature, including studies from the Naval Postgraduate School and NIST publications, this research will identify key inefficiencies in the current RMF process and propose targeted improvements. Specifically, the paper will examine gaps between expected and actual cybersecurity performance, streamline the Authority to Operate (ATO) process, and offer solutions aimed at improving both transparency and operational efficiency while reducing redundant efforts. In addition to addressing inefficiencies, this research will focus on enhancing RMF's adaptability to emerging technologies and the dynamic nature of modern threats. As cyber threats become more sophisticated and as the pace of technological innovation accelerates, a more flexible, forward-looking RMF is essential to maintaining operational security. The research will also explore how to integrate real-time threat intelligence and automation into the RMF process to further strengthen its capabilities. The expected outcome is a more agile and responsive RMF that better aligns with the DoD's evolving mission needs and technological advancements. The proposed revisions are intended to enhance joint integration, improve the overall cybersecurity posture, and increase operational effectiveness, ensuring the DoD's communication infrastructure remains secure, adaptable, and capable of responding to future challenges and adversarial threats.

Keywords: Department of defense (DoD), Department of the navy (DON), Risk management framework (RMF), National institute of standards and technology (NIST), Authority to operate (ATO)

1. Introduction

The Department of Defense's (DoD) use of its constructed communication infrastructure is essential to operate in today's environment to complete tasks from sharing information to enabling effective command and control. Protecting this infrastructure is vital to ensure that it serves as intended and that the hardening measures improve the security of the systems to acceptable levels. The DoD provides consistent hardening of the communication network. It addresses potential cyber security threats by ensuring that all technological systems meet the Risk Management Framework (RMF) requirements outlined by the National Institute of Standards and Technology (NIST). The RMF framework and related documents require that all technological devices and any Program of Record must meet the acceptable level of associated security and privacy controls before it is granted an Authority to Operate (ATO) on a DoD network (NIST, 2018). The NIST RMF is the guiding framework for ensuring information technology (IT) systems security and is a continuous process (U.S. Department of Defense [DoD], n.d.). The RMF was implemented in March of 2014 with the release of the publication "DoD Instruction (DoDI) 8510.01: Risk Management Framework for Information Technology" to replace the previous framework to complete the certification and authorization of systems, which was the DoD Information Assurance Certification and Accreditation Process (DoD, n.d.). The reason for the new process design was to provide a framework that would provide guidance and standards to standardize the process of information systems across all federal agencies and manage the cybersecurity risk throughout the system's life-cycle (DoD, n.d.). Although this paper does use literature that specifically focuses on challenges identified within the Department of the Navy's implementation, it is important to understand that the RMF policy applies to all services within the DoD; the challenges the authors discuss are intrinsic to the RMF and are the root cause of the issues with the RMF implementation within the Navy, which is why the authors incorporate literature from the DoD-wide perspective highlighting key themes.

[1]The views expressed here are those of the authors and do not necessarily represent the views of the Naval Postgraduate School, the Department of Defense, or the U.S. Government

As technology continues to develop and evolve, the system must be capable of quickly and efficiently adopting and implementing new technology at the speed of relevance. The ability to promptly leverage and integrate new and emerging capabilities is essential and helpful in maintaining the DoD's competitiveness and providing additional capabilities. The RMF process needs to support these demands to ensure the system works by increasing the cybersecurity posture and providing an objective and rapid means of getting ATOs approved. The current RMF process is subjective and consists of multiple workflow tools that cause an unnecessarily inconsistent ATO renewal process, which makes the process inefficient.

The problem is that the current RMF process is subjective, compliance-based, and an inefficient framework that does not effectively ensure information system security and cost-effectiveness through reciprocity. This is a problem because technology is rapidly evolving. As this technology continues to evolve and the DoD works toward more joint technological integration and solutions, the acquisition, implementation, and integration of equipment should not be hindered by the process due to its structure.

The purpose of this article is to analyze current issues with the RMF to provide recommendations that make the assessment criteria more objective, more efficient, and oriented towards threat-based security to ensure a more effective framework. This research is significant because it aims to identify ways to revise the current framework to ensure that the RMF process can meet the demands of future conflicts. This research will result in recommended revisions to the RMF process to bridge the gap between expected and actual information system security and provide a better-secured network.

This article will explore several research questions to determine the specific issues with the current implementation and structure of the RMF that prevent it from meeting the needs of the DoD regarding security, reciprocity, flexibility, and effectiveness. These research questions were generated from a comprehensive literature review, including theses of previous Naval Postgraduate School (NPS) students:

1. What are the current limitations of the RMF process?
2. How are these limitations preventing the RMF process from meeting the intent of its design?
3. How can the current RMF process be revised to address these deficiencies?

2. Literature Review

The Naval Postgraduate School (NPS) thesis by Bucks and Williams (2021), which involved researching the Marine Corps implementation of the RMF, provides insights into the challenges faced by the Marine Corps and maintaining a competitive advantage. Their study identified multiple issues, including the subjectivity of the RMF process and an over-reliance on a compliance-based approach that leads to a false sense of security within the DoD. Although Bucks and Williams's findings focused on the application within the Marine Corps, other services are experiencing similar challenges and limitations of the RMF. This study also discovered that the assessments conducted by the SCAs for systems include a significant degree of subjectivity. Bucks and Williams also uncovered that the assessment process focused on assessing and validating that the system owner implemented the security controls based on the ATO's approved controls rather than if the controls were effective or necessary for securing that system.

Another issue discovered through Bucks and William's (2021) research was "The lack of common security control implementations and documentation standards across the services combined with the fact that the Marine Corps uses its own separate RMF workflow tool, that does not share data about ATOs or evaluations elsewhere in DOD, creates significant inefficiencies and precludes the benefits that reciprocity would provide. Using a Marine Corps-specific tool for the A&A of all emerging technologies for use on the MCEN and DOD networks should not be a contributor to inefficiencies in our processes. Funding and development support for MCCAST is vital to improving the speed and efficiency of delivering capabilities to the warfighter and the Marine Corps ability to iterate faster than our adversaries" (Bucks & Williams, 2021, p. 44).

To provide context on the lack of a common centralized platform, the authors noted that every service except the Marine Corps uses the eMASS as their official RMF workflow tool; Instead of eMASS, the Marine Corps uses the Marine Corps Certification and Accreditation Support Tool (MCCAST) as their official RMF workflow tool (Bucks & Williams, 2021). It is important to note that the authors do explain that Marine Corps officials use eMASS when collaborating with other services, but it is an inefficient process due to the users needing to submit ATO documents within MCCAST manually afterward; the users need to submit the ATO documents manually because the two systems do not communicate with one another, and it is a wonder if the data structure is in place to enable the transfer of data without loss if those two systems could communicate. The findings of this study relate to the authors' research because they highlight the current issues with reciprocity,

efficiency, effectiveness, compliance, and subjectivity. The thesis findings inform the need for either a revision to the RMF or the creation and implementation of a new process across the DoD, specifically regarding the use of RMF workflow tools within the DoD.

Another NPS thesis relevant to the authors' topic is from Heier and Morales (2020) titled "Quantifying the Risk Management Framework." Heier and Morales explore the challenges that the DoD, specifically the Navy, will face with the current RMF structure and the evolving cybersecurity risks. The authors elaborate on the subjectivity of the RMF that they discovered during their research and the need for improvements and revisions to the RMF; the recommendation is that the process must be more objective and less subjective to increase standardization and cybersecurity. This thesis is relevant to the authors' topic because it outlines the subjectivity in the RMF process, how it impacts the decisions made towards security, and the lack of providing sufficient security measures and risk mitigation to the DoD's IT infrastructure, which ultimately hinders the security posture of the DoD (Heier & Morales, 2020).

The first article about subjectivity and its relation to risk perception is from Campbell (2006). The article covers the subjectivity and objectivity of risk and the perceived harm. Campbell notes that an individual or group's preferences and attitudes impact what that individual considers a risk, and considering their preferences and attitudes, the level of that risk determines what is considered harmful. The article presents different interpretations to demonstrate that risk can be subjective or objective depending on the scenario and instance. The author explicitly states, "Once your preferences are known, then whether there exists a risk, and how much of a risk there is, is a matter of objective fact" (Campbell, 2006, p. 227). This article is relevant to the authors' literature review because it demonstrates how risk can be subjective depending on the person and their preferences and attitudes, which can translate to differences in risk assessment and decisions. Also, once a person's thoughts and tolerance towards risk are known, they are an objective fact, especially towards other people within an organization, which are AOs in this case. This literature is important to the authors' problem because once someone's risk preferences are known, it enables a person to tailor a package for acceptance based on someone's preferences rather than ensuring the system is secure.

The article from Stevens et al. (2020) addresses compliance-based approaches to security by focusing on digital security compliance standards and whether they are effective at protecting against security concerns. The authors discovered in their research, "When compliance standards are used literally as checklists — a common occurrence, as confirmed by compliance experts — their technical controls and processes are not always sufficient. Security concerns can exist even with perfect compliance" (Stevens et al., 2020, p. 1). The authors claim these "controls and processes are not always sufficient" despite the emphasis on them because the efficacy of the compliance standards is not understood (Stevens et al., 2020, p. 1). The authors reinforce this point by stating, "While they may provide important security benefits, it is also possible that they lull security practitioners into a false sense of security, conflating high compliance audit scores with strong security. It is also possible that standards which are useful as general guidelines can become problematic when interpreted legalistically as checklist requirements" (Stevens et al., 2020, p. 1). This literature demonstrates the shortfalls of the RMF's compliance-based nature and its ability to meet the intent of improving cybersecurity.

The next literature piece that focuses on the issues presented by a compliance-based approach is the Department of the Navy's (DON) Cyber Strategy. The strategy discusses priorities and states that the way forward is to focus on cyber readiness and measures by "adhering to an operationally relevant, threat-informed process that affordably reduces risk and produces capabilities that remain secure after they have been delivered at speed" rather than strict compliance considering it has led to insecure systems, which is relevant considering the DON actively employs the RMF process (DON, 2023, p. 7). The DON wants to move towards a threat-informed and operationally relevant model while including compliance to ensure that systems are secure. The DON stated it needs to create a consistent method of measuring cybersecurity risk holistically. Also, the current process will transition to be effective at responding to threats by implementing real-time monitoring capabilities that can determine the effectiveness of implemented security controls, cyber hygiene, and adversarial assessments; The DON coined the term "cyber currency" to mean that a specific unit has followed the proper cyber guidance so they have earned the right to operate on the network, which is establishing credibility of doing the right cybersecurity measures based on the DON's guidance (DON, 2023, p. 7). Finally, the DON will begin integrating cybersecurity measures from the program's inception, ensuring that the systems engineering process occurs and that security is built into the system rather than added later to meet security requirements. This literature demonstrates that the DON is encountering issues with compliance and the acquisition process that leads to insecure systems. The shift from strict compliance to other means in the name of system security reinforces that the goal is secure systems, not a process or checklist.

Literature that addresses the efficiency of the RMF process within the DoD is from the DoD Office of Inspector General (2021) report titled "Audit of the DoD's Use of Cybersecurity Reciprocity Within the Risk Management Framework Process," which focuses on using reciprocity within the DoD. The audit's objective was to determine if the DoD was leveraging reciprocity to reduce the inefficient use of resources such as the assessments and work required for ATOs that already exist for the same or similar systems. The audit determined the DoD was not leveraging reciprocity.

In December 2017, the audit noted that the eMASS configuration control board added a feature to the registration processes that automatically identified all systems as a "reciprocity system." The audit also states that the DoD Chief Information Officer (CIO) provided a means to the users to exempt the system from the reciprocity requirement "if the system was classified or was being decommissioned" (DoD, Office of the Inspector General [IG], 2021, p. 5). Therefore, if the exemption is applied, it will not be visible to all users on eMASS, only "reciprocity users," which is what is currently happening and actively preventing sharing this information (DoD, Office of the IG, 2021). According to the audit, there is a system in place for users within the organization to be appointed as "Reciprocity Users," which means that the users appointed have read-only access to the documentation related to all the DoD systems in eMASS, regardless of if the "reciprocity system" designation was removed (DoD, Office of IG, 2021). The audit stated that the DoD CIO did not implement processes to oversee reciprocity, "instead the DoD CIO relied on DoD components to manage the system authorization process and use reciprocity to maximize reuse" (DoD, Office of IG, 2021, p. 8). The audit found that seven DoD components were not classifying systems as reciprocity systems in eMASS, although ATOs exist for those systems. The DoD IG audit illustrates that the systems in place to enable reciprocity within eMASS have failed, and the information discovered on the use of reciprocity within the DoD and in eMASS does not align with the RMF and its goal for increasing reciprocity and achieving resource efficiency.

The DoD CIO memorandum (2024) focuses on leveraging reciprocity within the RMF process; this memorandum addresses the inefficiencies in how services leverage reciprocity within the DoD. The memorandum explicitly states, "I expect testing re-use and reciprocity to be implemented except when the cybersecurity risk is too great. When Authorizing Officials cannot reach an agreement to leverage re-use and reciprocity, and cannot find resolution with the respective DoD Component CIOs, I direct that both parties engage directly with the DoD CIO to resolve the impasse" (Office of the Chief Information Officer, 2024, para. 3). This memorandum demonstrates that the DoD realizes that the organization is not using resources efficiently and the current reciprocity process and RMF is not operating as the DoD intended.

Ultimately, researching the effectiveness of the RMF is necessary to determine whether it makes systems more secure. The measures the RMF implements must be effective; otherwise, it is a process solely for optics. The authors will review several examples of literature and demonstrate how they relate to the problem outlined in this paper. Another piece of literature related to effectiveness is Buggenhout (2023), which focuses on implementing the concept of Purple Teaming instead of purely Blue Teams and Red Teams acting independently of one another performing their functions. Buggenhout claims that Blue and Red Teams work collaboratively to identify and fix vulnerabilities. The paper claims that the current method of using blue and red teams independent of one another creates a strained environment between the two teams by findings from the Red Team causing the Blue Team to become defensive. Also, purple teaming will ensure that the TTPs and attacks that the red team is using to penetrate the system are realistic and based on what the threat actor is for that scenario, as opposed to an over-sophisticated, effective attack that is unlikely to be what is encountered by the organization (Buggenhout, 2023).

Also, Buggenhout (2023) claims that integrating Breach and Attack Simulation tools into an organization's process enables continuous purple team activities, which increase the effectiveness and efficiency of the organization's resources. The author states that after a red team conducts a scenario, the organization can import that specific scenario and TTPs to automate the periodic execution of the scenario; The automation of the threat scenario enables the blue team to continue to encounter that scenario and their ability to respond, while enabling the red team to focus on other threat scenarios (Buggenhout, 2023). The article explores the use of automation and tools to streamline this process to reduce the strain on the budget and personnel requirements and enable continuous purple teaming activities, enabling the continuous monitoring aspect that the RMF attempts to achieve. A real-time approach to monitoring risk provides a better security posture than periodic assessments; ATOs perform periodic assessments yearly and only review the implementations of security and privacy controls within the ATO, as opposed to whether those controls are effective and the system can detect a breach. This literature is relevant because it presents the purple teaming concept as a solution to increase collaboration, the efficient use of resources through automation and tools, and makes the

teams more versatile in their craft, which increases security to a higher degree than compliance and more effectively meets the intent of the RMF.

In the article from Austin et al. (2019), the authors speak about the insecurities that arise from interface protocols that allow software and hardware to operate together. The authors give two reasons for why these protocols pose threats, which are that they "operate at least partially in kernel space" and are "commonly designed to accommodate a large and diverse set of interactions with legacy, current, and future systems alike" (p. 3). The authors state that the DoD primarily addresses vulnerabilities reactively, relying on an expedited cybersecurity observe, orient, decide, and act loop to identify, assess, and patch threats as they arise. The DoD continues this practice today and "attempts to use software updates to address more systemic issues are still the root cause of everything from loss of availability to loss of life" (Austin et al. 2019, p. 3). The authors claim that consensus is growing regarding the DoD taking a proactive approach, such as fielding systems “that are provably free of certain class of vulnerability” (Austin et al. 2019, p. 3).

The authors mention that the systems employed today use standardized protocols and interfaces that egregiously violate the principles of least privilege; however, the DoD depends on and uses these protocols and interfaces because they provide benefits to enable the interoperability and access to commercial off-the-shelf equipment and software (Austin et al., 2019). The authors state, "These protocols remain vulnerable despite the use of cybersecurity methodologies like the RMF" (p. 3). The authors use an example of the RMF's recommended control baseline for critical DoD systems that address interface security, including CM-7, SC-7, and SI-10 (Austin et al., 2019). The authors claim that the mentioned "controls can be implemented in a way that adheres to the principle of least privilege and protects a system from malicious input, in practice this is almost never the case" (Austin et al. 2019, p. 3). The authors use these controls and their application to explain why the RMF is ineffective (Austin et al., 2019). Finally, the authors state, "Two flawed assumptions underpin the assurances provided by the RMF. The first is the belief that security can be realized almost entirely through corrective actions (e.g., the real-time configuration management and monitoring prescribed by the above controls). The second is the belief that security can be asserted through subjective, human assessment of test and evaluation artifacts" (Austin et al. 2019, p. 4). The authors claim that using principled engineering practices removes the need for these assumptions because the systems are designed to provide a machine-checkable means of tracing the desired security properties from the system's design to its implementation, taking a proactive approach, rather than applying a reactive security approach of focusing on only handling issues as they appear (Austin et al., 2019).

Ultimately, the authors are advocating for an overhaul of the current RMF, and the methodology the DoD uses must shift away from a human-centric process and a reactive response approach to a proactive, automated, and design-oriented methodology. This literature is relevant because it demonstrates the ineffectiveness of the RMF in meeting the intent of ensuring the security of IT systems and the process and DoD policies promote "a stagnant culture of cybersecurity via compliance,” rather than promoting a culture that addresses the root causes of these cyber security issues (p. 3).

The final effectiveness literature is a report from the GAO. The GAO (2021) reviewed five acquisition programs with initial contracts awarded after the DoD implemented the RMF. The report discovered that three of these five programs did not have cybersecurity requirements outlined when awarded and had to be modified later to include the cybersecurity requirements. After being modified, only one of the contracts had detailed security requirements (GAO, 2021). The other two had generic cybersecurity statements that contractors interviewed by the GAO during the audit stated were common for requests for proposals from the government to include statements such as "comply with RMF" or "be cyber resilient." (GAO, 2021, p. 21). The lack of detailed requirements then filtered to the fact that there are no specific guidelines on measuring the effectiveness of the cybersecurity measures implemented for that program (GAO, 2021). With the lack of emphasis on specific requirements, it is easy to see how the programs are implementing or not implementing controls without fully understanding what the system needs, and unclear cybersecurity requirements negatively impact the DoD's ability to institute better security (GAO, 2021). This literature is directly relevant to the RMF because it demonstrates that there is no way, in some instances, such as the ones audited, to verify that the implemented controls reduced the risk to the system, which directly goes against the RMF's goal, and at minimum demonstrates the RMF has no way of demonstrating it’s current effectiveness.

3. Analysis

The prior research and literature available demonstrate that the current method that the RMF employs to address cybersecurity is inadequate to provide the best security posture possible. The DoD has done an

inadequate job of managing the current usage of RMF workflow tools. Every service within the DoD, except the Marine Corps, uses eMASS as the primary workflow tool. This workflow tool deviation is a problem, but addressing this problem alone will not fix the issue of ensuring the availability of reciprocity documentation. The DoD must mandate that the Marine Corps stop using MCCAST and formalize eMASS as their only RMF workflow tool. Also, eMASS must remove users' ability to apply the reciprocity system exemption unilaterally at the submitter level.

The DoD must employ stricter and more scrutiny measures, and this starts with establishing a process where an exemption is requested and approved by an individual far removed from the units and/or departments submitting the system packages into eMASS. The second analysis is that the current compliance-based approach is inadequate. The DoD must build information technology systems and software with security integrated from the beginning of the system/software development Life Cycle. The DoD will address the root problem of potential vulnerabilities and issues from the beginning by properly engineering systems with security built-in principles, thus increasing the overall security posture, as Austin et al. (2019) argued.

The RMF process introduces a significant amount of subjectivity into the process, and even though there are qualitative and quantitative aspects of risk management, the RMF must find the correct balance while employing the RMF structure (Chapple et al., 2021). For instance, In NIST's RMF, "the AO is the only person who can accept risk," so they must review the authorization package to determine the appropriate response and make an informed decision on the authorization of the ATO (NIST, 2018, p.72). There are no clear standards on what defines a system as secure, nor is there anything preventing an AO from issuing a denial of authorization to a reciprocity request approved by another AO. The lack of standards in this process actively prevents the efficient use of resources and actively introduces ambiguity, exacerbating current issues with the RMF.

4. Conclusion

As this paper noted, the RMF is a cornerstone of the Department of Defense's cybersecurity posture, but its current implementation is hindered by subjectivity, inefficiencies, and a compliance-driven approach that falls short of addressing evolving technological threats. Through an analysis of existing literature and operational challenges, this paper highlights critical gaps, including the lack of reciprocity, inefficiencies in the ATO process, and inadequate integration of threat-informed and proactive methodologies. Addressing these challenges requires a shift towards a more objective, standardized, and threat-driven framework that prioritizes real-time monitoring and automation.

Future research should focus on developing a comprehensive and measurable standard for assessing system security that minimizes subjectivity while enhancing consistency across services. Additionally, exploring the integration of advanced technologies such as artificial intelligence and breach-and-attack simulation tools could provide a path forward for continuous and dynamic risk management. Empirical studies are needed to validate the effectiveness of these tools in improving the RMF's ability to adapt to emerging threats. Finally, evaluating the feasibility of a unified RMF workflow tool across all branches of the DoD could streamline processes, reduce redundancies, and enhance joint operations.

By addressing these areas, the RMF can evolve into a robust, forward-looking framework capable of securing the DoD's critical infrastructure against the ever-changing cyber threat landscape. This transformation is essential to ensuring the DoD remains agile, resilient, and prepared to meet the challenges of the future.

References

Austin, E., Gagnon, R., Shull, A. and Templeman, R. (2019) 'Toward High-Assurance Interface Protocols for Department of Defense Applications (Op-Ed)', *Journal of DoD Research and Engineering: Special Edition*, 2(2), pp. 2–6..

Bucks, M.B. and Williams, D. (2021) *Maintaining a Competitive Advantage: An Analysis of the Efficiency and Effectiveness of the Marine Corps' Assessment and Authorization Process.* Master's thesis. Naval Postgraduate School.

Campbell, S. (2006) 'Risk and the Subjectivity of Preference', *Journal of Risk Research*, 9(3), pp. 225–242.

Chapple, M., Stewart, J.M. and Gibson, D. (2021) *ISC2 CISSP Certified Information Systems Security Professional Official Study Guide.* 10th edn. Sybex.

Department of Defense, Office of Inspector General (2021) *Audit of the DoD's use of Cybersecurity Reciprocity Within the Risk Management Framework Process.* Report No. DODIG-2022-041 [Redacted].

Department of the Navy (2023) *Department of the Navy Cyber Strategy.* U.S. Department of Defense.

Heier, M.I. and Morales, A.J. (2020) *Quantifying the Risk Management Framework.* Naval Postgraduate School.

International Organization for Standardization (2015) *ISO 9000:2015 - Quality management systems - Fundamentals and vocabulary.* ISO.

National Institute of Standards and Technology (2018) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy.* NIST Special Publication 800-37, Rev. 2. U.S. Department of Commerce.

Office of the Chief Information Officer (2024) *Resolving RMF Challenges to Improve Security Authorizations.* U.S. Department of Defense.

Stevens, R., Dykstra, J., Everette, W.K., Chapman, J., Bladow, G., Farmer, A., Halliday, K. and Mazurek, M.L. (2020) 'Compliance Cautions: Investigating Security Issues Associated with U.S. Digital-Security Standards', *Proceedings of the Network and Distributed System Security Symposium (NDSS)*.

U.S. Government Accountability Office (2021) *Weapon Systems Cybersecurity: Guidance Would Help DoD Programs Better Communicate Requirements to Contractors.* GAO-21-179.