Securing Commercial Satellites for Military Operations: A Cybersecurity Supply Chain Framework

Courtney Fleming, Mark Reith, and Wayne Henry
Air Force Institute of Technology, Wright-Patterson Air Force Base, USA

courtney.fleming@afit.edu
mark.reith@afit.edu
wayne.henry@afit.edu

Abstract: The increased reliance on commercial satellites for military operations has made it essential for the Department of Defense (DoD) to adopt a supply chain framework to address cybersecurity threats in space. This paper presents a satellite supply chain framework, the Cybersecurity Supply Chain (CSSC) Framework, for the DoD in the evaluation and selection of commercial satellite contracts. The proposed strategy is informed by research on cybersecurity threats to commercial satellites, national security concerns, current DoD policy, and previous cybersecurity frameworks. This paper aims to provide a comprehensive approach for safeguarding commercial satellites used by the DoD and ensuring the security of their supporting components. Inspired by the National Institute of Standards and Technology (NIST) 800-171 requirements and the DoD's future Cybersecurity Maturity Model Certification (CMMC) process, the two-part framework significantly streamlines the NIST requirements to accommodate small businesses. It also extends key NIST requirements to commercial-off-the-shelf (COTS) suppliers. The CSSC Framework complements the CMMC certification process by addressing the need for cybersecurity requirements for all subcontractors supporting a commercial space asset. The framework incorporates a scoring process similar to CMMC scoring, granting points to a subcontractor for meeting the cybersecurity requirements outlined by the framework. In addition, the framework creates a space architecture overview that details the overall bid score and establishes a matrix based on individual requirements. This model and matrix allow DoD acquisition personnel to closely analyze each contract bid, comparing the subcontractor's strengths and weaknesses to other bidders. The CSSC Framework will allow the DoD to apply NIST standards to subcontractors who do not meet the requirements for CMMC certification.

Keywords: Space Systems, Commercial Satellites, Supply Chain, Space Cybersecurity, Commercial-Off-The-Shelf

1. Introduction

In recent years, the commercial space industry has grown rapidly, making it easier and cheaper for businesses and academic institutions to deploy satellites in low-earth orbit. A domain that was once dominated by governments around the globe is now accessible to almost any type of organization. However, the market demand for these quickly deployable systems highlights a growing cybersecurity concern. Commercial satellite systems may require multiple vendors within a complex supply chain, many of which do not follow centralized, standard cybersecurity requirements. The DoD recognizes the importance of addressing cybersecurity in space systems and acknowledges the potential national security threats posed by supply chain risks. However, there is currently no framework outlining how the DoD can secure the space cybersecurity supply chain.

This paper proposes a Cybersecurity Supply Chain (CSSC) framework outlining the requirements that contractors and subcontractors within the space supply chain should follow in order to bid for a DoD contract. Before presenting the CSSC Framework, the paper first discusses cybersecurity threats to commercial satellites, including a recent state-sponsored attack on a US commercial satellite. This paper also examines recent research by the National Institute of Standards and Technology (NIST), the Aerospace corporation, and the MITRE corporation, as well as current DoD policy related to space, cybersecurity, and the supply chain. In addition, the paper briefly describes a general satellite architecture and uses this architecture to propose the two-part framework.

2. Cybersecurity threats to commercial satellites

Historically, commercial satellite developers have not prioritized cybersecurity considerations when creating space systems, similar to the challenges at the inception of the Internet. However, as the space domain's attack surface expands with the increase of satellites in orbit, experts are concerned with cybersecurity threats posed to commercial satellites, whether privately owned or used by the government (House of Representatives, 2022). For example, Falco (2019) highlights that satellites can be a single point of failure for entire industries. Additionally, the supply chain for space systems can be long and involve many stakeholders. The use of

commercial-off-the-shelf (COTS) software within these systems is also a concern. Furthermore, there is a lack of regulation and a need for space system cybersecurity standards when evaluating space products (Falco et al., 2022). These factors make satellites and their components vulnerable targets for adversaries, including state and non-state actors, to exploit. This is especially concerning as these single points of failure can affect communication, navigation, and imagery for millions of people.

The use of COTS software and hardware components presents unprecedented challenges for commercial satellites, as the presence of these assets in space has diversified from government control to CubeSats deployed by many businesses. COTS components allow companies and organizations to launch satellites at a low cost, but they also have the potential for vulnerable components due to fast production and little security consideration. The use of COTS components allows attackers to easily access the code to explore for vulnerabilities, which was previously more difficult when satellites used proprietary software (Nussbaum and Berg, 2020). Despite swift patches to discovered vulnerabilities, significant challenges impede patching to space systems in orbit, and many remain unpatched. Even though publicized attacks on in-orbit satellites are limited, cyber upkeep on ground-based components and strong network security for components in space is still a need (Nussbaum and Berg, 2020).

Similar to large technology companies, space systems face many of the same challenges as those in terrestrial cyberspace. One study analyzed satellite incidents between 1977 and 2019, categorizing them based on both the architecture and industry targets. Most attacks targeted the ground segment of government satellite architectures (Manulis et al., 2021). Manulis et al. (2021) further assessed that most of these attacks were conducted for state espionage, political gain, and corporate espionage, and employed techniques such as jamming, computer network exploitation, hijacking, and phishing. Over the last decade, the number of satellites in orbit increased exponentially, and the amount of satellite incidents follow this trend.

3. Recent example: state attack on US commercial satellite

As the DoD expresses its intent to incorporate commercial satellites into military operations, it is important to analyze cyber attacks aimed at these dual-use satellites to understand the threats imposed by near-peer adversaries. The most recent example is the Russian cyber attack in February 2022 on satellites of US company, ViaSat, which supported Ukrainian telecommunications during the Russia-Ukraine conflict. Boschetti et al. (2022) conducted an in-depth review of this cyber attack, highlighting its significance as the only publicly known attack against a commercial space system used by a government. While the details about the attack are unknown, Boschetti et al. (2022) present a hypothetical attack cycle based on statements made by ViaSat. In 2022, attackers exploited a vulnerability discovered years prior within the VPN “Fortigate”. Boschetti et al. (2022) further elaborate that the ViaSat attack began with the attacker using this unpatched VPN to access ViaSat ground segments, which were maintained by a subsidiary of another satellite company, to finally access ViaSat’s modem management interface. From there, the attackers uploaded wiper malware and disabled communications for thousands of users.

This attack demonstrates the need for vetting contractors to ensure their third-party provided components are secure, that the contractors use a zero-trust architecture, and that contractors practice quality vulnerability checks and patch management (Boschetti et al., 2022).

4. National security concerns

In July 2022, experts representing the MITRE Corporation, NIST, and the Aerospace Corporation testified in front of the Subcommittee on Space and Aeronautics, under the House Science, Space, and Technology Committee regarding satellite cyber threats to the United States. Their testimony expressed concern for cybersecurity attacks on satellites causing a collision with another satellite in-orbit. Specific examples of attacks affecting satellite operations include using an injection of malicious code to spoof sensor data, corrupt sensor systems, or unauthorized commands for guidance and control (House of Representatives, 2022). Their testimonies further outlined the criticality behind securing space systems. The Defense Intelligence Agency (DIA) assessed that foreign adversaries plan to target space systems through cyber operations. Current security limitations include a lack of a widely adopted technical standard for commercial space assets and a lack of information sharing within the research and development sector for space technology.

5. Recent research efforts

Researchers now acknowledge the threats to space cybersecurity and propose frameworks to address these threats. The Aerospace Corporation led the initiative to create the Space Attack Research and Tactic Analysis (SPARTA), a matrix based upon the MITRE Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK) framework, a knowledge base of tactics, techniques, and procedures (TTPs) demonstrated by adversaries to launch cyber attacks. The MITRE ATT&CK model lists and explains techniques for each stage of the cyber attack including reconnaissance, initial access, privilege escalation, command and control, and impact. It also lists mitigation measures and recommendations to combat the adversary's TTPs (MITRE Corporation, 2022). SPARTA mirrors MITRE's matrix and applies it to space cyber attacks, listing TTPs specific to space to gather information from the space and cybersecurity communities and fully address and share adversarial TTPs (SPARTA, 2022). Another characteristic unique to SPARTA is it incorporates references from NIST that outlines recommended countermeasure controls, which experts found most relevant to space. Both frameworks acknowledge that supply chain compromise is a tactic used by adversaries to gain initial access in order to aid a cyber attack.

Additional research efforts to address the threats in the space domain include a recent collaboration between NIST and the MITRE corporation to provide an existing cybersecurity framework for commercial space operators to apply to their systems. Scholl and Suloway (2022) outline their work as supporting Space Policy Directive 5 (SPD-5) which directs government agencies to define cybersecurity norms for those operating in the space domain. Their work describes the threats to commercial satellite systems and the Cybersecurity Framework created from Executive Order 13636, Improving Critical Infrastructure Cybersecurity. The functions within the framework are "identify, protect, detect, respond, and recover." Scholl and Suloway (2022) provide a matrix of subcategories supporting the five functions, which detail specific actions commercial satellite operators can take or self-evaluate to ensure their infrastructures are secure. NIST and the MITRE Corporation are still refining this product, and the actions listed within this research are only recommendations at this point.

6. Current DoD policy

Little information is available regarding the DoD's implementation of a space-specific cybersecurity framework to address supply chain threats. However, in December 2021 the DoD released the Cybersecurity Maturity Model Certification (CMMC) Version 2.0 Overview to provide an updated framework for protecting federal contract information and controlled unclassified information within the supply chain. The CMMC model measures the implementation of cybersecurity requirements based upon the Federal Acquisition Regulation (FAR) and NIST standards and divides these measurements into three levels: Level 1 consists of 17 "foundational" practices recommending an annual self-assessment of these practices. Level 2 consists of 110 "advanced" practices recommending triennial third-party assessments. The incomplete level 3 is intended to contain "expert" practices from NIST SP 800-172 for triennial government assessments (CMMC Model Overview, 2022). The CMMC model consists of 14 domains including, but not limited to, access control, awareness/training, identification/authentication, and security assessment. An example of practices by level under these domains is insider threat training, meeting the NIST 800-171 Rev 2 3.2.3 requirement, which is classified as a Level 2 practice under awareness/training (CMMC Model Overview, 2022). While contractors are already required to maintain cybersecurity standards outlined by NIST 800-171, COTS component suppliers are exempt from the CMMC certification requirement (General Services Administration, 2022). A survey of multiple businesses following the previous CMMC Version 1.0 model revealed that small businesses were more likely to struggle with the CMMC compliance (Strohmier et al., 2022).

Additionally, the DoD enforces policy regarding open-source/COTS software, which is useful when considering satellite software, such as flight software. The Office of the DoD Chief Information Officer (CIO) published answers to frequently asked questions relating to open-source software. The office asserts that it encourages the use of open-source and COTS software as it is generally inclined to be more secure due to more developers and reviewers being able to identify vulnerabilities, discrediting the "security by obscurity" theory (Office of DoD CIO, 2021). It frequently references a study from 2003 produced by MITRE, analyzing the use of open-source software in the DoD, which concludes that open-source software played a critical role in the DoD. Without it, there would be negative consequences, limiting the DoD from protecting its network (MITRE Corporation, 2003). For security, this study recommends that the DoD develop a list of open-source software that is "generally recognized as safe," but the DoD has not developed such a list. According to the Office of DoD CIO, the DoD requires commercial software to come with a warranty or source code to ensure the supplier or government can maintain the software.

For general DoD supply chain threats, the DoD published an action plan in response to Executive Order 14017 to address defense supply chains (US DoD, 2022). Its focus areas as most pressing to national security include kinetic capabilities, energy storage and batteries, castings and forgings, and microelectronics and include "cyber posture" as a strategic enabler, encompassing industrial security, counterintelligence, and cybersecurity. The document briefly mentions space as a supply chain concern, referencing spacecrafts as a platform containing cast and forged parts, but it lacks cybersecurity considerations.

7. Commercial satellite components/architecture

This section presents a brief overview of commercial satellite general components and architecture to fully understand the diversity of potential suppliers that support the architecture. Willis et al. (2017) describe a notional satellite as being similar to an industrial control system, made up of systems within systems connected via buses. The main elements within the architecture are propulsion, thermal, power, attitude, and data handling subsystems. Similarly, Scholl and Suloway (2022) provide an overall, general architecture of satellite operations which divides into three segments: the space segment, the ground segment, and the user segment. The space segment consists of a link sub-segment, internal satellite cybersecurity sub-segment, and a satellite-to-satellite communication sub-segment. The ground segment is terrestrial operations conducted by humans, which can be co-located with launch facilities, separate from these facilities, or outsourced altogether. The user segment describes the endpoints for the consumers such as GPS receivers, telecommunication equipment, and aircrafts. The following proposed framework omits the user segment and uses the space and ground segments described by Scholl and Suloway (2022) as a reference.

8. Proposed framework

This section proposes a notional framework for acquisitions to understand the contractor's supply chain from launch to orbit and outlines cybersecurity requirements that each of the contractor's suppliers must meet to bid for a DoD contract. Rather than relying on the CMMC model to ensure cybersecurity compliance, the CSSC Framework uniquely compliments the CMMC model by extending cybersecurity requirements to COTS suppliers. The CSSC Framework also applies to any contractor that supports the commercial satellite regardless of the contractor's likelihood to store or handle controlled unclassified information. The framework's supporting cybersecurity conditions are streamlined from the CMMC model, reducing the domains from 14 to five, to overcome the complexity of a long supply chain with multiple COTS suppliers. The five domains are network management, identification/authentication, system management, general security, and incident prevention/response. The new domains combine and summarize the requirements outlined in the CMMC model while meeting the key provisions of NIST 800-171. Also similar to the CMMC certification process, the framework implements a scoring system which provides an overall "bid score", consisting of a summation of the sub-scores from the five requirement categories. Like the CMMC certification process, the CSSC Framework requires a self-assessment and a third-party assessment before a contract bid submission. The following subsections explain the criteria for each of the five domains.

8.1 Network management

This domain focuses on the subcontractor's ability to properly enact security measures within all networks that the subcontractor owns or any other networks interfacing with the subcontractor's networks. Some of the concerns within the category include remote access, open ports, and secure protocols, which can lead to vulnerabilities if these network features are not properly configured. The CMMC Model Overview (2022) inspired this category. The framework summarizes requirements affecting the network and includes lessons learned from the ViaSat attack (Boschetti et al., 2022), resulting in four requirements. First, a company needs a zero-trust network architecture and must demonstrate how it verifies and controls connections to external networks as necessary. A third-party assessment may evaluate the strength of the zero-trust architecture. A supplier must also have a Virtual Private Network (VPN) connection in place, from a reputable provider, for wireless, mobile, and remote access that also prevents split tunneling. Network managers must also disable nonessential ports, protocols, and services, implementing a "least functionality necessary" approach to the networks. Finally, company networks need a policy that denies network communications traffic by default and allows traffic by exception.

8.2 Identification and authentication

This domain evaluates how well the subcontractor enforces identification and authentication practices for anyone attempting to access its systems or networks. The domain combines requirements from the "Identification and Authentication" and "Audit and Accountability" domains from the CMMC Model Overview (2022), which results in four requirements. First, the company needs a multifactor authentication technique. One effective example is issuing physical dongles to users that generate a random key to enter for system access in addition to using a smart card to plug into a terminal. For password implementation as part of multifactor authentication, the system must require a level of complexity and periodical changes with no repeating passwords while maintaining practical usability. Additionally, the company establishes a limit on unsuccessful login attempts, and the system must keep a log of unsuccessful login attempts. All systems and websites maintained by the company may only store and transmit cryptographically protected passwords, meaning the system must have an effective, non-proprietary hashing algorithm that obscures user passwords. Lastly, any systems and websites shall obscure stored authentication information. At a minimum, usernames and passwords cannot be stored in clear text.

8.3 System management

This domain focuses on the subcontractor's ability to properly enact security measures within all systems that the subcontractor owns. Adopted from multiple domains of the CMMC Model Overview (2022), primarily "System and Communications Protection" and "System and Information Integrity", there are seven requirements aligned with NIST 800-171. The company demonstrates the limitation of information system access based on absolute "need-to-know" or "need-to-access" principle of authorized users. Also, privacy and security notices/banners must be present during a user's initial system access to assist in incident response. All systems need automatic session locks and termination after a reasonable period. Any information technology products require established security configuration settings within the organizational system. System managers must configure only essential capabilities for organizational systems, adopting a "least functionality necessary" approach. Similar to the network management policy requirement, systems must enforce a "deny-all, permit by-exception" policy for the installation and execution of software within the system. Lastly, the subcontractor must demonstrate routine maintenance procedures and file scanning for systems periodically.

8.4 General security

This domain encompasses requirements that implement overall cyber-secure policies and practices. This includes training, media handling, physical security, and hardware screening, summarizing multiple domains from the CMMC Model Overview (2022). The six requirements include a company's implementation of routine training and awareness for role-based risk/responsibilities, insider threats, elicitation, phishing attacks, and media handling. The company also needs a policy for media handling, marking, accountability, and disposal. Within facilities, employees are required to easily identify authorized personnel to screen individuals on the premise. In the event an employee is terminated or re-assigned to another position, security managers re-evaluate and/or remove all identification characteristics, permissions, and accesses to systems following duty changes. Additionally, the company requires general facility security practices to include escort procedures, access logs, and additional barriers to screen for authorized personnel continuously. Finally, as applicable for critical hardware, the supplier/design team must ensure there are quality assurance inspections through design and use of hardware to identify defects or counterfeit components.

8.5 Incident prevention and response

This domain requires subcontractors to ensure any actions taken on networks, systems, and individual accounts are logged and analyzed while also ensuring these actions can be correctly attributed to the suspect user account. The seven requirements primarily summarize the "Incident Response" domain from the CMMC Model Overview (2022). System and network managers must conduct routine analysis and monitoring of audit logs for suspicious and unauthorized use. System capabilities require the synchronization of internal system clocks for audit records. Networks and systems must trace any actions back to a unique user. The company needs an established policy outlining detection, analysis, containment, and recovery incident-handling capabilities if there is suspicion that an intrusion occurred within the organization's systems. The contractor requires an incident reporting plan to notify all affected stakeholders and appropriate officials. Company cybersecurity professionals must conduct internal vulnerability scans and search for vulnerabilities published in open-source forums that

affect the organization. Lastly, software managers shall employ reputable static and analysis tools to look for vulnerabilities within the organization's software.

The first part of the CSSC Framework presents a way for a major company with multiple subcontractors under them to clearly outline the supply chain involvement so the DoD can properly vet them. This part also lists the suppliers' overall bid scores and affiliated foreign countries involved in the suppliers' operations. The foreign country affiliation requirement allows the DoD to ensure components do not originate from near-peer adversaries, and that an adversary does not influence a company's work with the DoD. Figure 1 depicts a supplier overview that the contractor would provide to the DoD, based on the satellite architecture described by Suloway and Scholl (2022). The framework divides the suppliers into two categories: the ground segment and the space segment. The ground segment is further divided into three subcategories: mission operations center, payload control center, and bus interfaces. Rather than divide the mission operations buses and payload buses into their own subcategories, all buses and links are compiled into one subcategory for brevity. Each subcategory lists the supporting supplier. For example, in Figure 1 Supplier C and Supplier D provide hardware and software that support the payload control center. In this scenario, any suppliers who provide communication capabilities from the ground segment to the space segment are classified under "bus interfaces."

Similarly, the space segment is divided into three subcategories: hardware components, embedded software, and internal communication. Each subcategory lists the supporting supplier. In Figure 1, for example, Supplier H and Supplier I provide software for the satellite's embedded systems. Any bus interfaces within the satellite are classified under "internal communication." The figure depicts an example of the number of suppliers supporting the overall commercial satellite architecture, and this number may vary. Additionally, a supplier may provide more than one function. For instance, a supplier supporting the mission operations center could also supply a component supporting the payload control center.

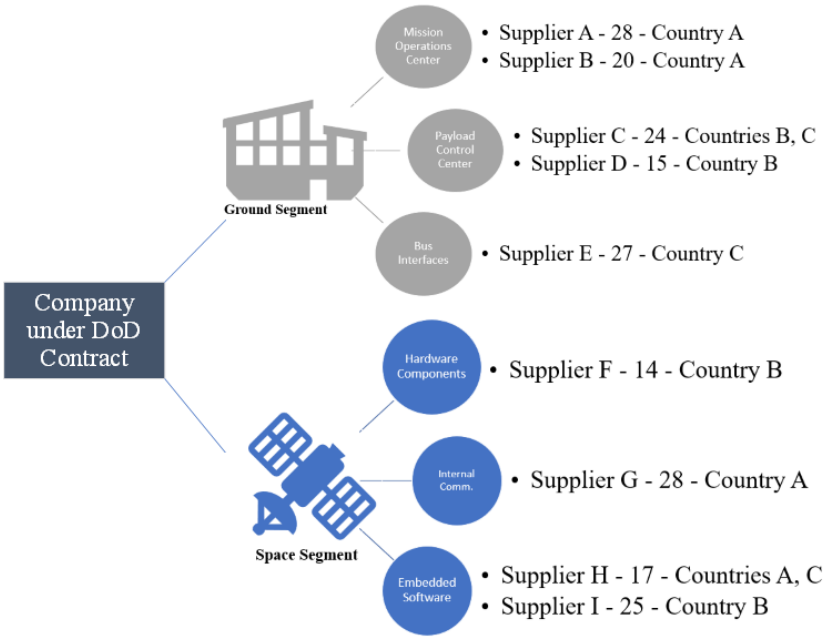

Figure 1: An overall depiction of each supplier providing services to the DoD contractor. This overview divides into the ground and space segments, listing the main capabilities of each segment. Each supplier providing the capability has an associated overall bid score and affiliated foreign countries providing support to the company.

Each supplier in every subcategory has an overall bid score. The scores are based on each requirement listed within the five domains supporting the underlying framework. If a supplier meets a requirement, it receives one point. Suppliers may not receive any points for partially satisfied requirements. The maximum bid score a supplier may receive is 28 points. In Figure 1, Suppliers A and G have a bid score of 28, meaning it has satisfied all cybersecurity requirements within each domain. Every supplier also has its affiliated foreign countries, and in Figure 1, countries B and C provide operational or financial support to Supplier C.

The second part of the CSSC Framework outlines a matrix for DoD acquisitions personnel to evaluate the supplier's strengths and weaknesses within each domain. The matrix is color-coded green, yellow, and red to symbolize domain requirement compliance. If the supplier meets all requirements within a domain, its cell is green. If the supplier meets over 50% of the requirements within a domain, its cell is yellow. For failing to meet 50% or more of the requirements, a supplier's cell is red. Figure 2 represents a matrix to accompany the example provided in Figure 1. Since Suppliers A and G have a perfect bid score, all their cells are green. The red cells in the "Hardware Components" row indicate Supplier F failed to meet more than 50% of the requirements in network management, identification/authentication, and system management. However, the yellow cells in the same row show that Supplier F met between 50% and 100% of the requirements in general security and incident prevention/response. Through the example used in Figure 2, an acquisition officer may deem a contractor is unsuitable considering the overall incident prevention/response requirement deficiencies.

	Network Management	Identification and Authentication	System Management	General Security	Incident Prevention and Response
Mission Operations Center	Supplier A	Supplier A	Supplier A	Supplier A	Supplier A
	Supplier B	Supplier B	Supplier B	Supplier B	Supplier B
Payload Control Center	Supplier C	Supplier C	Supplier C	Supplier C	Supplier C
	Supplier D	Supplier D	Supplier D	Supplier D	Supplier D
Bus Interfaces	Supplier E	Supplier E	Supplier E	Supplier E	Supplier E
Hardware Components	Supplier F	Supplier F	Supplier F	Supplier F	Supplier F
Internal Communication	Supplier G	Supplier G	Supplier G	Supplier G	Supplier G
Embedded Software	Supplier H	Supplier H	Supplier H	Supplier H	Supplier H
	Supplier I	Supplier I	Supplier I	Supplier I	Supplier I

Figure 2: A matrix demonstrating the strengths and weaknesses of each supplier's compliance for each domain. The matrix is color-coded to reflect the level of compliance for the requirements outlined in the domains. This provides a depiction to acquisition personnel of the cybersecurity viability for the space asset.

The benefits of the two-part framework include the enforcement of the NIST 800-171 standards for any contractor or subcontractor, including COTS suppliers. Additionally, the extension of these standards to all contractors, regardless of controlled unclassified information handling, mandates strong business practices and cybersecurity principles if they want to work with the DoD. The CSSC Framework also reduces the 127 requirements outlined in Levels 1 and 2 of the CMMC Version 2.0 model to 28 requirements. This alleviates the budgeting and planning overhead for small businesses who already struggle with the CMMC certification process. Lastly, the DoD acquisitions personnel reviewing the contract bid may use the framework for a detailed visual representation of the overall space architecture. DoD experts can compare the strength of each bidder's space and ground segments and its components, identify overall domain deficiencies, and understand the foreign countries tied to each subcontractor for supply chain threat management.

9. Limitations and future work

While there are several ways to evaluate the effectiveness of the CSSC Framework, open-source research is scarce since commercial satellite websites advertising their product do not provide a full list of their suppliers. Additionally, it is difficult to evaluate how well these suppliers implement cybersecurity practices unless there is publicly available information that reports negative publicity such as intrusions or data theft. Future research may find practicality in working directly with contractors and their suppliers/subcontractors to evaluate this proposed supply chain framework. However, there may be challenges in collaborating with suppliers due to their reluctance to publicly disclose possible vulnerabilities in their information technology infrastructure. As a result, research on this topic may be limited to distribution within the DoD only.

Among the several ways to evaluate the framework effectiveness is addressing the balance between enforced cybersecurity principles and the supply chain's ability and willingness to propose a bid that complies with these standards. One question to consider is whether the CSSC Framework requirements are too loose or unrealistic for subcontractors to follow, especially for COTS suppliers. A survey of commercial satellite COTS suppliers would help answer this question. Another consideration is the implementation of a DoD-led inspection to evaluate compliance. For example, the CMMC Model Overview (2022) enforces annual or tri-annual inspections by

government or third-party entities. A concern for a complex supply chain is having adequate DoD manpower to inspect every supplier or if more inspections are needed due to commercial satellites' mission-essential capabilities. An additional factor to consider is a comparison between this streamlined framework and the CMMC 2.0 model. While the CSSC Framework is intended to compliment the CMMC 2.0 certification process, future work could analyze if the framework eliminates critical requirements from the CMMC 2.0 model.

10. Conclusion

The space domain was previously restricted to state governments, and only a few decades ago, there were not as many deployed satellites in low-earth orbit. Commercial nanosatellites now clutter low-earth orbit, and it only increases the attack surface for cyberattacks against space systems. The DoD wants to use commercial satellites to facilitate its intelligence and detection capabilities. However, a framework and standard for cybersecurity within the space supply chain is missing to ensure the DoD can operate safely in space as it relies on commercial satellite operators. This paper proposes a two-part framework that enables transparency within the commercial space supply chain and outlines requirements that contractors and suppliers must meet to compete for a contract. The paper also recommends ideas and challenges for future researchers to evaluate the CSSC Framework and compare it to an existing DoD cybersecurity framework.

Disclaimer

The views expressed are those of the authors and do not reflect the official policy or position of the US Air Force, Department of Defense, or the US Government.

References

Aerospace Corporation. (2022). *Software Dependencies & Development Tools, Technique IA-0001.01 | SPARTA.* [online] Available at: https://sparta.aerospace.org/technique/IA-0001/01/.

Boschetti, N., Gordon, N.G. and Falco, G. (2022). Space Cybersecurity Lessons Learned from The ViaSat Cyberattack. In ASCEND 2022 (p. 4380).

Falco, G. (2019). Cybersecurity principles for space systems. Journal of Aerospace Information Systems, 16(2), pp.61-70.

Falco, G., Henry, W., Aliberti, M., Bailey, B., Bailly, M., Bonnart, S., Boschetti, N., Bottarelli, M., Byerly, A., Brule, J. and Carlo, A. (2022). An International Technical Standard for Commercial Space System Cybersecurity-A Call to Action. In ASCEND 2022 (p. 4302).

General Services Administration. (2022). 252.204-7021 Cybersecurity Maturity Model Certification Requirements. | Acquisition.GOV. [online] Available at: https://www.acquisition.gov/dfars/252.204-7021-cybersecuritymaturity-model-certification-requirements.

House of Representatives. (2022). *Exploring Cyber Space: Cybersecurity Issues for Civil and Commercial space systems: House Committee on Science, Space and Technology*. [online] Available at: https://science.house.gov/hearings/exploring-cyber-space-cybersecurity-issues-for-civil-and-commercial-space-systems.

Manulis, M., Bridges, C.P., Harrison, R., Sekar, V. and Davis, A. (2021). Cyber security in new space. International Journal of Information Security, 20(3), pp.287-311.

MITRE Corporation. (2022). *MITRE ATT&CK*. [online] Available at: https://attack.mitre.org/.

MITRE Corporation. (2003). Use of Free and Open-Source Software (FOSS) in the U.S. Department of Defense. [online] Available at: https://dodcio.defense.gov/Portals/0/Documents/FOSS/dodfoss_pdf.

Nussbaum, B. and Berg, G. (2020). Cybersecurity implications of commercial off the shelf (COTS) equipment in space infrastructure. Space infrastructures: From risk to resilience governance, pp.91-99.

Office of the DoD Chief Information Officer. (2021). *Open Source Software FAQ.* [online] Available at: https://dodcio.defense.gov/open-source-software-faq/#q-is-oss-commercial-software-is-it-cots.

Scholl, M. and Suloway, T. (2022). Introduction to Cybersecurity for Commercial Satellite Operations (2nd Draft), *National Institute of Standards and Technology*.

Strohmier, H., Stoker, G., Vanajakumari, M., Clark, U., Cummings, J. and Modaresnezhad, M. (2022). Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base. JOURNAL OF INFORMATION SYSTEMS APPLIED RESEARCH.

United States Department of Defense (DoD). (2022). *Cybersecurity Maturity Model Certification (CMMC) Model Overview*. [online] Available at: https://www.acq.osd.mil/cmmc/docs/ModelOverview_V2.0_FINAL2_20211202_508.pdf.

United States Department of Defense (DoD). (2022). *Securing Defense-Critical Supply Chains.* [online] Available at: https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF.

Willis, J.M., Mills, R.F., Mailloux, L.O. and Graham, S.R. (2017). Considerations for secure and resilient satellite architectures. In 2017 International Conference on Cyber Conflict (CyCon US) (pp. 16-22). IEEE.