AEROSPACE REPORT NO.
TOR-2023-02161 - REV A

Space Segment Cybersecurity Profile for National Security Systems – Revision A

April 23, 2024

Brad V. Roeher[1], Paul J. de Naray[2], Brandon T. Bailey[3], Daniel P. Faigin[4]
[1]Cyber Assessments and Research Department, Cybersecurity and Advanced Platforms Subdivision
[2]Pentagon and Multi-Domain Division, Defense Strategic Space
[3]Cybersecurity and Advanced Platforms Subdivision, Information Systems and Cyber Division
[4]Cyber Operations and Resilience Department, Cybersecurity and Advanced Platforms Subdivision

Prepared for:

Department of the Defense Chief Information Office – Cybersecurity Integration
United States Department of Defense
6000 Defense Pentagon
Washington, D.C. 20301

Contract No. FA8802-19-C-0001

Authorized by: Defense Systems Group

Abstract

We present a cybersecurity profile approach to defining and performing threat-focused risk assessment for a space system space segment. The described cybersecurity profile approach significantly leverages content openly published within The Aerospace Corporation's (Aerospace's) Space Attack Research and Tactic Analysis (SPARTA) framework to show rationale for tailoring of the Committee on National Security Systems Instruction (CNSSI) No. 1253 space platform overlay. This threat-focused analysis creates unique tailoring of the space platform overlay and helps to provide a notional maximum control baseline from which system security engineering can more efficiently define cybersecurity requirements before a contract is set. We also present a notional minimum control baseline for national security systems that is based on SPARTA notional risk scores. This minimum baseline approach helps space segment acquisitions if they do not have resident expertise for control tailoring. All controls referenced in the baselines have example acquisition requirements on the SPARTA website to aid creating contracts, guiding development, and informing accurate assessments of control implementations.

Contents

Figures

Tables

1. Introduction

This is a revision to the original TOR-2023-02161 that was published on December 14, 2023.

Cybersecurity control baselines and overlays are a current method to define cybersecurity protections that manage system risks. Specifically for a space segment domain (i.e., space platform, spacecraft, space vehicles [SVs]), Aerospace's analysis has determined that common, current default control baselines and overlays have significant challenges with providing an efficient and sufficient space segment cybersecurity approach. This is likely driven by these default baselines having assumptions to serve general purpose computing needs across the cybersecurity community and this does not match with space segment assumptions. Aerospace analysis has shown that tailoring a default CNSSI No. 1253 [1] control baseline for a space segment requires significant effort to justify numerous control removals and this approach does not by default include critical additional controls necessary to counter space segment cyber threats. These two aspects indicate that a default CNSSI 1253 baseline tailoring approach will not scale well for numerous and varying space segments across the space enterprise and will leave systems vulnerable to modern threats.

The space segment "cybersecurity profile" approach in this document works to enhance default control baselines and overlays with a set of space segment scoped knowledge with risk-specific rationale that provides accurate control baseline tailoring. The content is provided with the intent to allow for more efficient implementation of the risk management framework (RMF) as defined in National Institute of Standards and Technology (NIST) special publications (SP) 800-37 [2]. Within wider cybersecurity framework considerations, there is also the NIST Cybersecurity Framework (CSF) Version 1.1 [3] to create profiles. This document does not specifically create a CSF profile; however, the content herein may be used to prioritize, scope, orient, and conduct risk assessments for CSF profiles.

Within the context of CSF, we must acknowledge the NIST interagency report (IR) 8270 [4] for commercial satellite operations. The NIST IR 8270 follows the CSF 1.1 process to create a profile via core functions, categories, and subcategories that identify associated "Informative References" controls from NIST SP 800-53 [5]. Aerospace analysis has found the NIST IR 8270 CSF control selection poorly addresses space segment specific risks described in this document. We theorize that the risk mitigation mismatch may be due to the CSF 1.1 informative reference controls being selected from CSF default assumptions that are more closely aligned with enterprise information technology system protection. Whatever the rationale for the CSF control mismatch, the guidance provided in this document should be utilized to understand control selection risk rationale more clearly.

Ultimately, this cybersecurity profile serves two primary purposes: (1) to enrich space segment cybersecurity knowledge and (2) to set more specific bounds on a space segment tailored control baseline. This profile leverages the existing CNSSI 1253 Attachment 2 to Appendix F, "Space Platform Overlay," but enhances the content with additional tailoring and justification. This enrichment is built off a history of Aerospace space system engagement and system security engineering that has cultivated a knowledge set represented in this profile. Additional space system cybersecurity knowledge exists on the SPARTA website at https://sparta.aerospace.org [6]. This cybersecurity profile provides a new maximum and minimum set of controls to consider for a space segment baseline. An overlay is presented to remove controls based on risks not being applicable through vulnerability assumptions and adds controls based on threat knowledge from SPARTA.

2. Scope and Approach

This document defines a profile approach to guide security control and enhancement (hereafter referred to as “control”) tailoring that can protect national security systems (NSS) or similar capabilities operating in space. The scope of this profile is specific to the *space segment* and related *link segment* portions of a broader *space system*. The basic segments of a space system are shown in Figure 1.

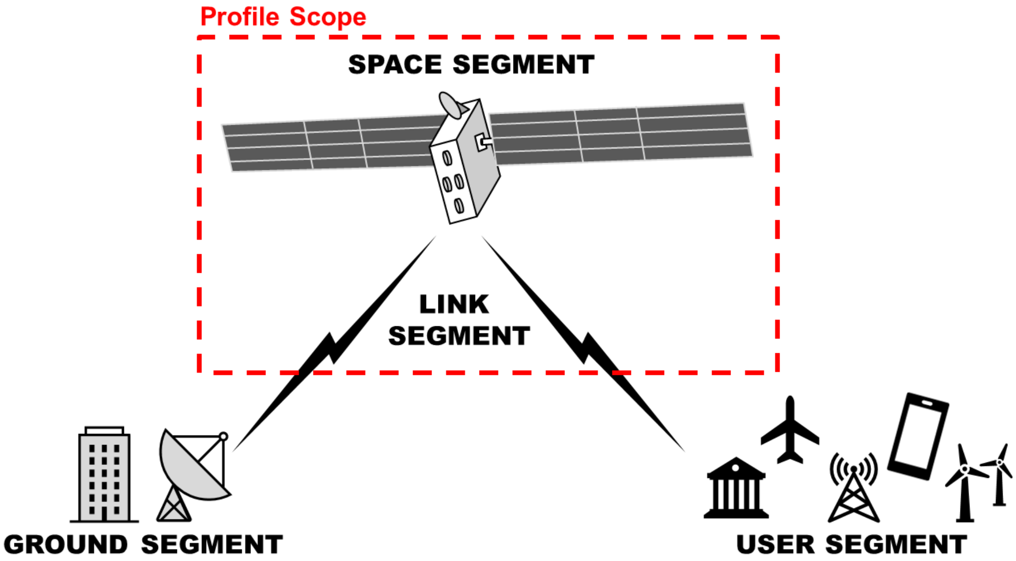
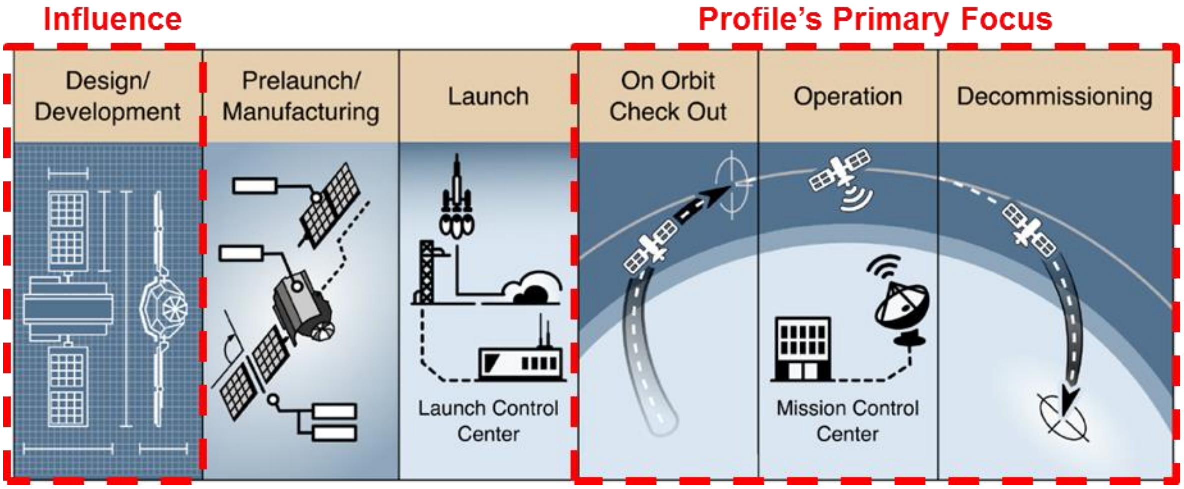


Figure 1 – Basic Space System Segments

The space segment includes the satellite platform, satellite payload(s) (e.g., communication, imaging, positioning navigation and timing), and onboard computer systems. The link segment includes communication between the space and ground (control and user segments); the components that enable the communication (e.g., antennas, transceivers); and data encryption, decryption, and transmission security components. This profile’s scope considers only the space segment’s interface with the link segment, which means that ground or user and link segment interface portions are not included (e.g., ground/user antennas, ground/user transceivers, ground/user encryption). Hereafter, the term “space segment” is used to mean both the defined space segment and the related portions of the link segment. The ground segment includes the ground station (e.g., command and control, data processing), ground network infrastructure, software development/sustainment, and cybersecurity operations. The user segment includes end-user devices, ground communication gateways, and user applications (e.g., navigation, remote sensing analysis).

An additional consideration for this profile is the applicable portions of the system development lifecycle (SDLC). There are many frameworks to describe an SDLC, but a good reference for this space segment context is the SDLC phases described in NIST IR 8270 [4]. These life cycle phases are shown in Figure 2 and this figure is used to indicate that the profile’s scope and influence across the SDLC. This profile’s primary focus is on cybersecurity controls during on-orbit checkout, space operations, and decommissioning. For systems security engineering (SSE) system segmentation consideration and to ensure appropriate segment responsibilities, this profile specifically excludes capabilities implemented in the ground and user segments that include the development environment, manufacturing environment, and launch. However, the space segment capabilities in this profile still influence design and development choices at the start of the SDLC because those capabilities are built on the ground. The early SDLC influence of this profile is further explained in Section 2.4.

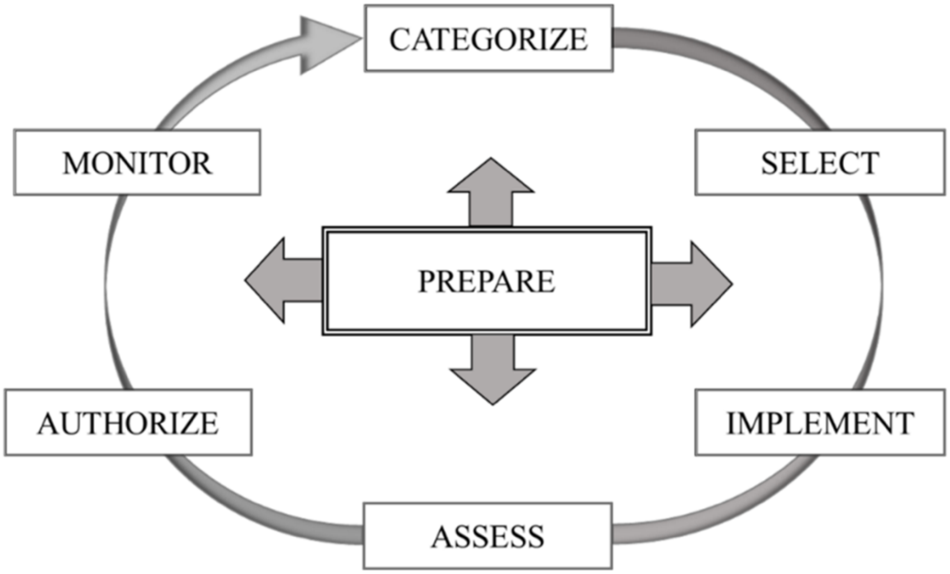


Courtesy of NIST

Figure 2 – Profile Coverage of Space Segment SDLC Phases

The cybersecurity profile in this document follows the NIST RMF [2] process and focuses on risk mitigation primarily driven by threats. The overall intent of this profile is to provide a portion of the knowledge and guidance that supports SSE efforts across a space SDLC. While this cybersecurity profile covers control baseline tailoring to drive requirements definition and system design in a larger space system, this profile does not cover the entire SDLC. For example, this profile does not include the controls necessary for the space segment software development environment and hardware manufacturing. Nonetheless, the controls and risk rationale provided in this profile still informs testing and evaluation procedures within the design and development phase.

The RMF manages risks within a cybersecurity process shown in Figure 3. The early portion of the process includes the upper right quadrant that involves SSE effort to shape system requirements and supports cybersecurity being an enabler of mission success. This profile's guidance is focused on the RMF Prepare, Categorize, and Select steps at both an organization and a mission level. Organization-level guidance creates artifacts and decisions to manage cybersecurity risk across the space segment enterprise. The



Courtesy of U.S. Department of Defense

Figure 3 - RMF Process Steps Illustration

organization-level guidance supports mission-specific Categorize and Select decisions for their cybersecurity needs. While much of this profile's guidance is for organization-level space segment needs, there is much detail provided on notional mission cybersecurity.

For the basics on the RMF process steps in this guidance, the Prepare effort scopes and characterizes risk, the Categorize step is to determine an initial impact-driven control baseline, and the Select effort is to tailor that control baseline for appropriate risk mitigations. While this guidance is focused on these three steps, the knowledge provided from this effort is beneficial across the SDLC. For example, as previously mentioned the risk knowledge can be utilized with test and evaluation design and this matches with the Assess RMF step.

From a Department of Defense (DoD) perspective, DoD instruction (DoDI) 8510.01 [7] provides clarity with more detailed tasks in each RMF step. The content provided in this profile supports the Prepare, Categorize, and Select tasks identified in Table 1. A core aspect of this cybersecurity profile is to provide space segment organization risk assessment (Task P-3) content to create organizationally tailored control baselines and profiles (Task P-4). The additional tasks supported in Table 1 will be identified in the subsequent sections for different risk assessment considerations.

Table 1 - RMF Step Tasks Supported by This Profile

Task	**Description**	**Profile Support**
PREPARE		
P-2	Risk Management Strategy	Establish risk tolerance
P-3	Risk Assessment – Organization	Complete organization-wide risk assessment through threats and vulnerabilities
P-4	Organizationally – Tailored Control Baselines and CSF Profiles	Tailored control baselines are established and made available
P-6	Impact-Level Prioritization	Prioritization of organizational space segments with the same impact level
P-15	Requirements Definition	Security requirements defined for control baseline
CATEGORIZE		
C-2	Security Categorization	Security categorization of the system to bound impact levels for control baseline selection
SELECT		
S-1	Control Selection	Select control baselines to protect against space segment risk
S-2	Control Tailoring	Tailoring control baselines specifically for space segment risk

2.1 Risk Assessment

In seeking to utilize a common nomenclature for risk, this profile leverages aspects of NIST SP 800-30 [8]. Risk impact is the magnitude of harm that can be expected from the compromise of a system's confidentiality, integrity, or availability. Risk likelihood is an analysis of the probability that a threat can exploit a vulnerability. The combination of impact and likelihood determines risk and Figure 4 illustrates these factors in a basic risk assessment approach. A more complex examination of threat, vulnerability, exploitability, existing countermeasures, and other detailed factors for a specific mission are not factored into the risk assessment in this profile. These more complex likelihood factors should be considered for tailoring under a mission's specific and complete risk assessment. Further detail on how to develop a complete risk assessment process is provided in NIST SP 800-30.

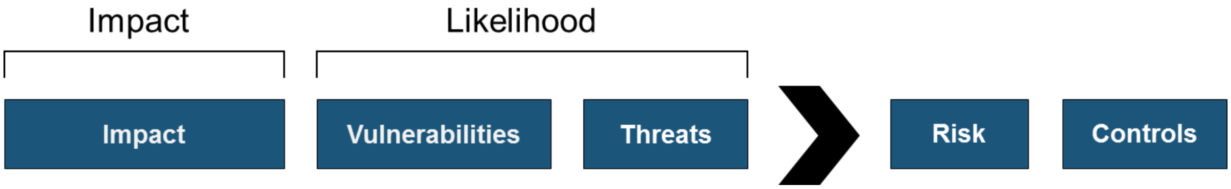


Figure 4 - Basic Risk Assessment Process

Risk ratings determined from an assessment must be considered under a risk management strategy and organization or mission risk tolerance (Task P-2). Risk tolerance influences risk mitigation decisions because a main goal of risk management is to mitigate risks below the defined risk tolerance threshold. Risk is mitigated by selecting cybersecurity controls that lower risk likelihood and therefore lower a risk rating below the defined risk tolerance threshold. A higher risk tolerance means that more operational risk is acceptable, and this generally means fewer controls will need to be implemented to mitigate the risk levels to below the risk threshold. Likewise, a lower risk tolerance encourages the implementation of more controls to mitigate risk levels to below the acceptable amount of risk. It should be noted that just selecting a greater number of controls will not guarantee risk mitigation. Risk mitigation is effective when a risk's threat and vulnerability considerations are linked to control mitigations. This profile provides the additional knowledge for linking threats and vulnerabilities to controls and this provides appropriate risk mitigation rationale for the space segment.

Impact can be determined by the RMF categorization Task C-2 based on Federal Information Processing Standards Publication 199 [9] impact categories. This impact categorization can be utilized to identify CNSSI 1253 control baselines that consider confidentiality, integrity, and availability compromise impact. This impact-based control baseline selection primarily accomplishes the selection Task S-1. The impact considerations in this profile present upper and lower boundary groupings for space segment impact and risk tolerance in line with the prepare Task P-6. Section 3 addresses a notional maximum tailored control baseline based on a high-impact NSS space segment with lower risk tolerance. Section 4 addresses a notional minimum tailored control baseline based on a moderate-impact NSS space segment with higher risk tolerance.

2.2 Vulnerability Tailoring

Vulnerability analysis is the examination of system weakness that can be exploited by a threat. Within a space segment context, this aspect is leveraged to remove controls based on applicability assumptions. If conditions are not applicable to the space segment, then there is no system weakness that can be exploited by a threat. For example, there are no human, physical operations on the spacecraft and therefore there are no human-related maintenance controls required. These assumptions enable a default control baseline from CNSSI 1253 to be tailored by removing controls that are not applicable to the space segment (Task S-2). The assumptions described in Section 3.2 were informed by previous assumptions listed in the CNSSI 1253, Attachment 2 to Appendix F, but this tailoring has been updated for space technology advances and newer possible adversary techniques.

It should be noted that these vulnerability assumptions and tailoring are focused on a distinction of the space segment from the ground segment. While this can help with clarity on separate control baselines to guide the implementation of cybersecurity protections, it is not intended for overall system cybersecurity to treat each segment in complete isolation. It is recommended that an SSE view is taken where there is a control implementation responsibility in each segment of a space system to addresses specific risks for that segment. There are also control implementations that are shared between segments because there is shared responsibility for a complete system solution. However, shared controls should not be interpreted as control inheritance where one segment provides protections for the other segment. Previous cybersecurity approaches have had an overreliance on control inheritance protection from the ground segment for the space segment. This profile defines the controls that are specifically the responsibility of the space segment. SSE efforts should define those controls that are shared between segments. Our goal is to provide shared control guidance in a separate document.

2.3 Threat Tailoring

A threat is any circumstance or event with the potential to adversely impact assets or operations via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service. Moving further into *threat events*, these have the potential to cause undesirable consequences or impact in the space segment. Threat events can be represented in the concept of tactics, techniques, and procedures (TTPs). Tactics represent the categorization of "why" a technique is used by a threat event, techniques and sub-techniques are "how" the threat event occurs, and procedures are the detailed implementation of a technique or sub-technique.

The characterization of threat events through TTPs can be helpful for risk assessment threat modeling analysis because TTPs provide detailed information for the threat analysis. A full set of space segment TTPs are on the Aerospace SPARTA website at https://sparta.aerospace.org. The large amount of content in SPARTA will not be repeated in this profile but will instead be referenced. This space segment profile describes the risk assessment process to leverage SPARTA TTPs and tailor control baselines (Task S-2). This also allows for the website to be the most current source for TTP knowledge and avoids unnecessary updates to this profile for less substantial updates.

A core aspect of this profile's analysis will be based on SPARTA techniques and sub-techniques. It should be made clear that formal, validated threat intelligence should be leveraged whenever possible. While these threat intelligence products should be authoritative for defining applicable threats to a space segment, sometimes these products lack the details necessary for linking threat products to specific SPARTA techniques. Every effort should be made by SSE analysis to match actual threat intelligence to techniques. If there is a lack of threat intelligence detail, then it is up to the SSE analysis to derive likely techniques that could be applicable to the space segment based on the specific mission and technical capabilities. SPARTA includes a set of threats to consider if SSE analysis is deriving applicable techniques. As shown in Figure 5, threat analysis and linkage are the starting point for selecting appropriate SPARTA techniques.

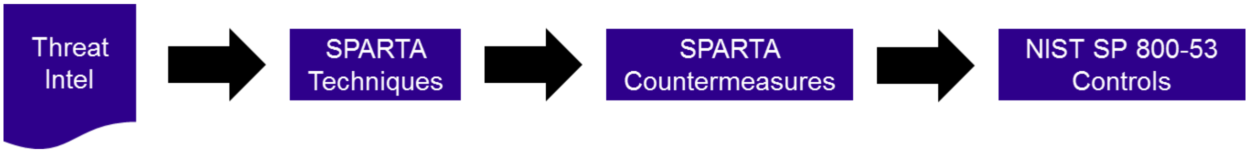
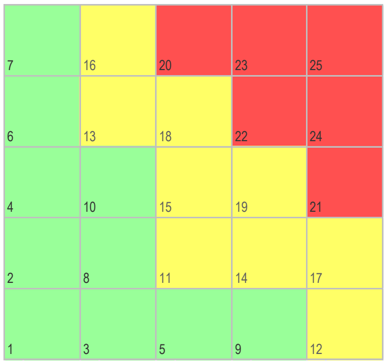


Figure 5 - Threat Linkage to Controls

Within SPARTA, all techniques are linked to mitigating countermeasures that represent security concepts and classes of technologies that can be used to prevent a technique or sub-technique from being successfully executed. These SPARTA countermeasures serve as an intermediary between techniques and control standards such as NIST SP 800-53 or the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) 27001 [10]. For the purposes of this profile, the selection of techniques and sub-techniques (hereafter referred to as "techniques") serve as the primary factor to determine the associated NIST SP 800-53 controls that are linked through countermeasures.

For risk assessment and mitigation below the notional maximum tailored control baseline, SSE should individually assess all identified space segment threats and determine risk ratings. Coupling the ratings with a risk tolerance threshold can then enable further tailoring of the control baseline to include only those risks that must be mitigated. Such a method was used to determine the notional minimum tailored control baseline in Section 4.

A knowledge set in SPARTA provides notional risk scores for each technique based on a notional “criticality” rating. In this process, criticality is a measure of the degree to which an organization depends on the success of the mission and is used to influence impact and likelihood ratings. SPARTA notional risk scores were determined by Aerospace subject matter expertise through estimating impact and likelihood numbers (i.e., 1-5) for each SPARTA technique, which then allows for each technique to be placed on a 5x5 matrix as shown in Figure 6. Specifically for likelihood determinations, the criticality factor was included by considering the attractiveness of a technique based on the difficulty of exploitation, adversary motivation, and adversary capability. A higher space segment criticality raises the attractiveness, likelihood, and ultimate risk of a technique. The 5x5 cell locations have fixed score numbers and colors that enable ordering and prioritization of all techniques based on risk. The technique risk scores above a risk threshold will provide a list of risks that must be mitigated. This technique list risk can then be used to pull in associated countermeasures and linked controls. This approach can effectively further tailor the notional maximum tailored control baseline into a more specific control baseline. This method was used to determine the notional minimum tailored control baseline in Section 4.



🟩 7	🟨 16	🟥 20	🟥 23	🟥 25
🟩 6	🟨 13	🟨 18	🟥 22	🟥 24
🟩 4	🟩 10	🟨 15	🟨 19	🟥 21
🟩 2	🟩 8	🟨 11	🟨 14	🟨 17
🟩 1	🟩 3	🟩 5	🟩 9	🟨 12

Figure 6 - Notional Risk Score 5x5

2.4 Acquisition Requirements

A primary goal for these SSE efforts should be to ensure that the tailored control baseline is directly utilized to create acquisition requirements. Without referencing detailed cybersecurity requirements in a request for proposal and subsequent contract, this leads to ambiguity in final cybersecurity risk mitigation and typically causes cybersecurity capabilities to not be appropriately funded by a contract. To enable cybersecurity requirements to be appropriately considered for a contract, SSE should identify all controls required by a tailored control baseline and requirement *shall* statements should be created to address these controls (Task P-15). Representative requirements are provided on the Aerospace SPARTA website to assist in the creation of control *shall* statements and to address threat rationale for why each requirement is needed to mitigate risk.

3. Notional Maximum Tailored Control Baseline

3.1 Impact and Risk Tolerance

Considering the NSS definition that includes intelligence activities, cryptologic activities, command and control of military forces, and weapon systems, these systems could and most likely will have higher impact from a compromise and this drives higher risk ratings. We acknowledge that there can be a lower-impact NSS space segment under consideration, and this should be handled by SSE effort that performs detailed risk assessment with associated risk tolerance selection. NSS will usually have lower risk tolerances due to the national security domain implications caused by a compromise.

Considering these combined aspects of likely higher impact and lower risk tolerance in risk management, the notional maximum control baseline selected in this profile would be a CNSSI 1253 High/High/High (H/H/H) control baseline for confidentiality, integrity, and availability, respectively. The H/H/H baseline is the largest control set defined by CNSSI 1253 and contains 573 controls. A more accurate starting control baseline should be further determined through control tailoring based on risk assessment with vulnerability and threat analysis.

3.2 Risk Assessment: Vulnerability Tailoring

Risk assessment tailoring based on space segment vulnerability is leveraged to remove controls based on the assumptions listed in Table 2. These assumptions enable the default control baseline from CNSSI 1253 H/H/H to be tailored through removing controls not applicable to the space segment. The result of the vulnerability tailoring is a removal of 263 controls from the H/H/H baseline and these are listed in Appendix A.

Table 2 - Vulnerability Assumptions

CONSTRAINED RESOURCES	Due to limitations in space segment size, weight, and power resources, space segments are not general-purpose systems. There are limitations on on-vehicle storage and transmission bandwidth. Some processing that might be done on the vehicle is often performed by the ground segment as a result.
NO PHYSICAL MAINTENANCE	Once deployed on orbit, human physical access for maintenance is not possible. This assumption does not preclude robotic access, which is continuing to emerge as a potential risk that must be evaluated.
NO REMOVABLE MEDIA	The space segment does not have removable media that is accessible during operation.
NO USER ACCOUNTS	Architecture does not utilize user accounts for identification and authentication specifically for space segment.
NON-TRADITIONAL NETWORKING	Although a space system may use TCP/IP protocols for ground communication transport and even possibly within a space platform bus, the space segment command and control does not utilize traditional networking capabilities. Space segment command and control does not directly interact with the Internet. This assumption is specifically separate from mission payloads that provide terrestrial users with separate satellite communications (SATCOM) capabilities.
NON-TRADITIONAL WIRELESS	All communications with the space segment are inherently wireless, but not in the sense of ground-based network wireless access points. Therefore, the controls intended to mitigate traditional wireless threats and vulnerabilities are either not applicable or implemented differently to address space-specific threats, vulnerabilities, and technologies.

NOT GENERAL PURPOSE	Due to the operational nature and environment, as well as resource limitations for size, weight, and power, systems operating in the space segment should not be considered general-purpose systems. System functionality focuses on the specific mission, leaving general-purpose or ancillary functions to the ground segment.
SPACE ENVIRONMENT	Risks arising from terrestrial or human-created disasters (e.g., fire, flood, and earthquake) do not apply for the space platform. Further, space segments do not operate in traditional information technology facilities with risks such as site security, fire detection and suppression, or flood or water damage detection. However, the space environment does introduce unique environmental hazards such as space weather resulting in impact caused high-radiation effects. These space environment specific threats are considered in the control baseline tailoring.
UNCREWED	The space segment's scope is for uncrewed platforms, so any direct personnel interaction is not possible. The threats from crew personnel access are not applicable to the space segment and controls are instead implemented by the ground segment.
USER TRAINING	Operational components within the space segment are not typically involved in the training of system users. Most controls dealing with user training are focused on implementation within ground segment applications and procedures.

3.3 Threats

As previously described, threats are factored into the risk assessment tailoring through threat events represented in SPARTA techniques. For the purposes of this unclassified, maximum tailored control baseline there are not any specific linkages to intelligence community threat intelligence products. Instead, all techniques applicable to the space segment in SPARTA were selected with their associated NIST SP 800-53 controls linked through countermeasures. Eighty-three additional unique controls are added to the space segment tailored control baseline and they are listed in Appendix B.

3.4 Notional Maximum Tailored Overlay

The summation of this risk assessment tailoring is shown in traditional overlay table in Appendix C. This overlay summarizes what controls should not generally apply to a space segment based on vulnerability and what controls could apply based on possible threats. This tailored baseline helps to tailor the default CNSSI 1253 H/H/H baseline from 573 controls down to a notional maximum of 393 controls.

4. Notional Minimum Tailored Control Baseline

4.1 Risk Assessment

In the context of NSS the definition of a minimum tailored control baseline still includes the importance of a space segment supporting NSS, but there will be considerations for lower impact and higher risk tolerance. As previously described in the process for risk scores, there is consideration for notional criticality of a space segment for NSS. The minimum impact of an NSS space segment would be a notional criticality of "medium" under the SPARTA risk score descriptions. A notional "low" criticality is for academic or research systems, while a notional "high" criticality correlates with the notional maximum tailored control baseline in Section 3. A notional medium criticality aligns with a strategy for civil, science/weather, commercial, or similar systems that are NSS or support NSS. While this approach provides a notional tailored control baseline to utilize as a minimum, it must be emphasized that additional countermeasures may be needed depending upon system-specific technologies, capabilities, or missions.

Through the process described in Section 2.3, the SPARTA notional risk scores in the 5x5 risk matrix cells have assigned colors as shown in Figure 6. For this notional minimum tailored control baseline, a higher risk tolerance would be a threshold that correlates with mitigating only risks that are red, which are those scores greater than 20 in the medium criticality category. The selection of techniques that match this risk threshold of scores greater than 20 are shown in Appendix D.

It should be noted that two techniques in the minimum tailored baseline techniques were removed based on additional analysis: EXF-0004 (Out-of-Band Communications Link) and EX-0001.02 (Bus Traffic). EXF-0004 was removed because the missions in the medium criticality do not likely utilize these out-of-band communication paths (e.g., cryptographic rekeying). EX-0001.02 was removed because an execution of this attack is difficult to accomplish on orbit as it requires direct access to the satellite bus interface and this capability is more complex of a compromise to execute.

Following Section 2.3 further, these tailored baseline techniques identify a set of possible mitigating countermeasures. However, just as the techniques above were tailored based on a higher risk tolerance threshold, these associated countermeasures were also tailored under that approach. The countermeasures listed in Table 3 were tailored out of the notional minimum tailored baseline.

Table 3 - Countermeasures Removed from Minimum Techniques

Counter-measure	Title	Rationale for Removal from Minimum NSS Baseline
CM0001	Protect Sensitive Information	Sensitive design information not stored in the space segment.
CM0004	Development Environment Security	Development environment does not exist in the space segment.
CM0005	Ground-based Countermeasures	Ground segment countermeasure.
CM0050	On-board Message Encryption	Unnecessary for higher risk tolerance.
CM0055	Secure Command Mode(s)	Unnecessary for higher risk tolerance.
CM0066	Model-based System Verification	Unnecessary for higher risk tolerance.
CM0067	Smart Contracts	Unnecessary for higher risk tolerance.
CM0068	Reinforcement Learning	Unnecessary for higher risk tolerance.
CM0069	Process White Listing	Unnecessary for higher risk tolerance.
CM0070	Alternate Communications Paths	Unnecessary for higher risk tolerance.
CM0072	Protocol Update / Refactoring	Unnecessary for higher risk tolerance.

CM0074	Distributed Constellations	Minimum baseline is for single SV design.
CM0075	Proliferated Constellations	Minimum baseline is for single SV design.
CM0080	Stealth Technology	Unnecessary for higher risk tolerance.
CM0082	Deception and Decoys	Unnecessary for higher risk tolerance.
CM0084	Physical Seizure	Unnecessary for higher risk tolerance.
CM0086	Filtering and Shuttering	Unnecessary for higher risk tolerance.
CM0087	Defensive Dazzling/Blinding	Unnecessary for higher risk tolerance.

The remaining countermeasures considered for this tailored baseline are shown in Appendix E. As a final step in the tailoring process, all controls linked to the tailored countermeasures are shown in Appendix F. It should be noted that this is a notional “minimum” tailored baseline to provide guidance in this profile for bounds on NSS space segment cybersecurity. This tailored baseline can be extended to other domains that support NSS, such as commercial space systems.

5. Conclusion

An NSS space segment cybersecurity profile comparison summary is shown in Figure 7. This figure shows how the quantity of default baseline controls is lowered through vulnerability tailoring and then additional necessary controls were added based on space segment specific threats. This figure also shows how SSE control tailoring can be utilized to create a notional minimum set of controls based on risk assessment effort. Both tailored baselines show how SSE effort can accomplish both efficient and sufficient cybersecurity protection for space segment needs.

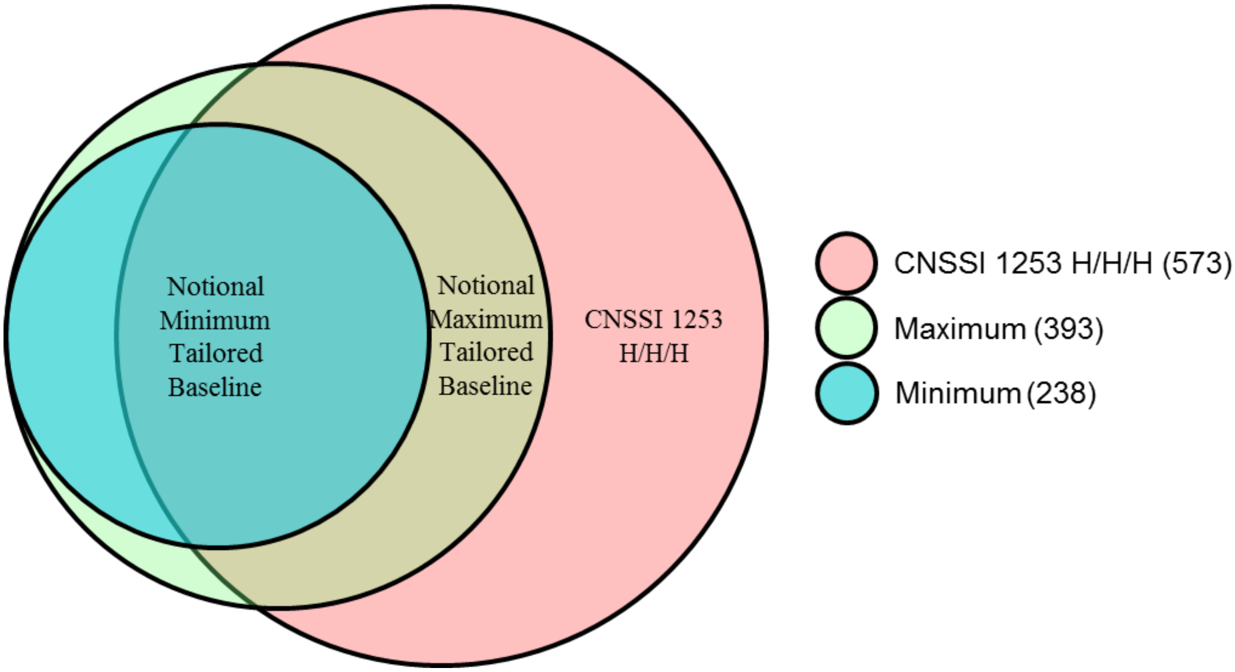

Notional Minimum Tailored Baseline
Notional Maximum Tailored Baseline
CNSSI 1253 H/H/H
CNSSI 1253 H/H/H (573)
Maximum (393)
Minimum (238)

Figure 7 - Venn Diagram of Notional NSS Space Segment Maximum and Minimum Tailored Control Baselines

References

1. Committee on National Security Systems (CNSS), *Security Categorization and Control Selection for National Security Systems*, CNSS Instruction No. 1253, Fort Meade, MD, July 29, 2022, https://www.cnss.gov/CNSS/issuances/Instructions.cfm

2. Joint Task Force, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37 Revision 2, Gaithersburg, MD, December 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf, https://csrc.nist.gov/pubs/sp/800/37/r2/final, https://doi.org/10.6028/NIST.SP.800-37r2.CSF

3. National Institute of Standards and Technology (NIST), *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, NIST CSWP 6, Gaithersburg, MD, April 16, 2018, https://csrc.nist.rip/pubs/cswp/6/cybersecurity-framework-v11/final, https://doi.org/10.6028/NIST.CSWP.04162018.

4. Scholl, M., and T. Suloway*, Introduction to Cybersecurity for Commercial Satellite Operations*, National Institute of Standards and Technology (NIST) Interagency Report (IR) 8270, Gaithersburg, MD, July 25, 2023, https://csrc.nist.gov/pubs/ir/8270/final, https://doi.org/10.6028/NIST.IR.8270.

5. Joint Task Force, *Security and Privacy Controls for Information Systems and Organizations*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 5 (includes updates as of December 10, 2020), Gaithersburg, MD, September 23, 2020, https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final, https://doi.org/10.6028/NIST.SP.800-53r5.

6. "Space Attack Research and Tactic Analysis (SPARTA)," Version 1.5.1, The Aerospace Corporation, November 29, 2023, https://sparta.aerospace.org.

7. Office of the Department of Defense (DoD) Chief Information Officer, *Risk Management Framework (RMF) for DoD Systems*, DoD Instruction 8510.01, Washington, D.C., July 19, 2022, https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf.

8. Joint Task Force Transformation Initiative, *Guide for Conducting Risk Assessments*, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 Revision 1, Gaithersburg, MD, September 17, 2012, https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf, https://csrc.nist.gov/pubs/sp/800/30/r1/final, http://dx.doi.org/10.6028/NIST.SP.800-30r1.

9. National Institute of Standards and Technology (NIST), *Standards for Security Categorization of Federal Information and Information Systems*, Federal Information Processing Standards (FIPS) Publication 199, Gaithersburg, MD, February 2004, https://csrc.nist.gov/pubs/fips/199/final, https://doi.org/10.6028/NIST.FIPS.199.

10. International Organization for Standardization/International Electrotechnical Commission (ISO/IEC), *Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements, Third Edition*, ISO/IEC 27001, Geneva, Switzerland, October 2022.

Appendix A – Controls Removed by Vulnerability Assumptions

Table 4 shows the controls removed by each vulnerability assumption. There is an additional column “Prev. Space Overlay” added to show how each removal relates to the previous CNSSI 1253 Attachment 2 to Appendix F, Space Platform Overlay, was applied to the CNSSI 1253 from March 27, 2014. In the overlay column, a “--" identified a control generally not applicable to that 2014 H/H/H baseline. It is acknowledged that the previous CNSSI 1253 Space Platform Overlay was developed in reference to NIST SP 800-53 Revision 4, which is different than this profile’s reference to NIST SP 800-53 Revision 5.

Table 4 - Controls Removed by Vulnerability Assumptions

Vulnerability Assumption	Control	Title	Prev. Space Overlay
CONSTRAINED RESOURCES	AC-19(5)	Full Device or Container-Based Encryption	
	AU-6(5)	Integrated Analysis of Audit Records	
	AU-11	Audit Record Retention	
	AU-11(1)	Long-Term Retrieval Capability	
	CM-2(3)	Retention of Previous Configurations	
	SI-2(2)	Automated Flaw Remediation Status	
	SI-2(3)	Time to Remediate Flaws and Benchmarks for Corrective Actions	
	SI-2(4)	Automated Patch Management Tools	
	SI-4(23)	Host-Based Devices	
	SI-15	Information Output Filtering	
NO PHYSICAL MAINTENANCE	MA-1	Policy and Procedures	
	MA-2	Controlled Maintenance	
	MA-2(2)	Automated Maintenance Activities	
	MA-3	Maintenance Tools	
	MA-3(1)	Inspect Tools	
	MA-3(2)	Inspect Media	
	MA-3(3)	Prevent Unauthorized Removal	
	MA-3(4)	Restricted Tool Use	
	MA-3(5)	Execution with Privilege	
	MA-3(6)	Software Updates and Patches	
	MA-4	Nonlocal Maintenance	
	MA-4(1)	Logging and Review	
	MA-4(3)	Comparable Security and Sanitization	
	MA-4(4)	Authentication and Separation of Maintenance Sessions	
	MA-4(6)	Cryptographic Protection	
	MA-4(7)	Disconnect Verification	
	MA-5	Maintenance Personnel	
	MA-5(1)	Individuals without Appropriate Access	

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	MA-6	Timely Maintenance	
	MA-6(1)	Preventive Maintenance	
	PE-5	Access Control for Output Devices	--
	PE-8	Visitor Access Records	--
	PE-8(1)	Automated Records Maintenance and Review	
	PE-8(3)	Limit Personally Identifiable Information Elements	
	SA-3(3)	Technology Refresh	
	SA-4(10)	Use of Approved PIV Products	
	SA-22	Unsupported System Components	
	SC-15	Collaborative Computing Devices and Applications	--
	SR-11(2)	Configuration Control for Component Service and Repair	
NO REMOVABLE MEDIA	AC-20(2)	Portable Storage Devices — Restricted Use	
	MP-1	Policy and Procedures	
	MP-2	Media Access	--
	MP-6	Media Sanitization	
	MP-6(1)	Review, Approve, Track, Document, and Verify	
	MP-6(2)	Equipment Testing	
	MP-6(3)	Nondestructive Techniques	--
	MP-7	Media Use	
NO USER ACCOUNTS	AC-2	Account Management	
	AC-2(1)	Automated System Account Management	
	AC-2(2)	Automated Temporary and Emergency Account Management	
	AC-2(3)	Disable Accounts	
	AC-2(4)	Automated Audit Actions	
	AC-2(5)	Inactivity Logout	
	AC-2(7)	Privileged User Accounts	
	AC-2(9)	Restrictions on Use of Shared and Group Accounts	
	AC-2(11)	Usage Conditions	
	AC-2(12)	Account Monitoring for Atypical Usage	
	AC-2(13)	Disable Accounts for High-Risk Individuals	
	AC-6(1)	Authorize Access to Security Functions	
	AC-6(2)	Non-Privileged Access for Non-Security Functions	
	AC-6(5)	Privileged Accounts	
	AC-6(7)	Review of User Privileges	
	AC-6(8)	Least Privilege Levels for Code Execution	
	AC-6(10)	Prohibit Non-Privileged Users from Executing Privileged Functions	
	AC-7	Unsuccessful Logon Attempts	

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	AC-10	Concurrent Session Control	
	AU-9(4)	Access by Subset of Privileged Users	
	AU-9(6)	Read-Only Access	
	AU-14	Session Audit	
	AU-14(1)	System Start-Up	
	AU-14(3)	Remote Viewing and Listening	
	AU-16(1)	Identity Preservation	
	IA-2	Identification and Authentication (Organizational Users)	
	IA-2(1)	Multifactor Authentication to Privileged Accounts	
	IA-2(2)	Multifactor Authentication to Non-Privileged Accounts	
	IA-2(5)	Individual Authentication with Group Authentication	
	IA-2(6)	Access to Accounts — Separate Device	
	IA-2(8)	Access to Accounts — Replay Resistant	
	IA-2(12)	Acceptance of PIV Credentials	
	IA-4(4)	Identify User Status	
	IA-5(1)	Password-Based Authentication	
	IA-5(2)	Public Key-Based Authentication	
	IA-5(8)	Multiple System Accounts	
	IA-5(16)	In-Person or Trusted External Party Authenticator Issuance	
	IA-8	Identification and Authentication (Non-Organizational Users)	
	IA-8(1)	Acceptance of PIV Credentials from Other Agencies	
	IA-8(2)	Acceptance of External Party Credentials	
	IA-8(4)	Use of Defined Profiles	
	IA-11	Re-Authentication	
	IA-12	Identity Proofing	
	IA-12(1)	Supervisor Authorization	
	SA-8(27)	Human Factored Security	
	SI-4(20)	Privileged Users	
NON-TRADITIONAL NETWORKING	AC-6(3)	Network Access to Privileged Commands	
	AC-17(3)	Managed Access Control Points	--
	SA-8(17)	Secure Distributed Composition	
	SC-7(3)	Access Points	
	SC-7(4)	External Telecommunications Services	
	SC-7(7)	Split Tunneling for Remote Devices	--
	SC-7(8)	Route Traffic to Authenticated Proxy Servers	--
	SC-7(15)	Networked Privileged Accesses	+
	SC-7(25)	Unclassified National Security System Connections	

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	SC-7(28)	Connections to Public Networks	
	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	
	SC-21	Secure Name/Address Resolution Service (Recursive or Caching Resolver)	
	SC-22	Architecture and Provisioning for Name/Address Resolution Service	
	SI-4(22)	Unauthorized Network Services	
NON-TRADITIONAL WIRELESS	AC-18	Wireless Access	
	AC-18(1)	Authentication and Encryption	
	AC-18(3)	Disable Wireless Networking	
	AC-18(4)	Restrict Configurations by Users	
	AC-18(5)	Antennas and Transmission Power Levels	--
	SI-4(14)	Wireless Intrusion Detection	
	SI-4(15)	Wireless to Wireline Communications	
NOT GENERAL PURPOSE	AC-4(4)	Flow Control of Encrypted Information	
	AC-8	System Use Notification	
	AC-16	Security and Privacy Attributes	
	AC-16(6)	Maintenance of Attribute Association	
	AC-16(7)	Consistent Attribute Interpretation	
	AC-21	Information Sharing	
	AC-22	Publicly Accessible Content	--
	AC-23	Data Mining Protection	
	AU-6(3)	Correlate Audit Record Repositories	
	AU-6(6)	Correlation with Physical Monitoring	
	AU-7	Audit Record Reduction and Report Generation	--
	AU-7(1)	Automatic Processing	--
	AU-12(1)	System-Wide and Time-Correlated Audit Trail	--
	AU-16	Cross-Organizational Audit Logging	
	AU-16(2)	Sharing of Audit Information	
	CM-6(1)	Automated Management, Application, and Verification	
	CM-6(2)	Respond to Unauthorized Changes	
	CM-7(3)	Registration Compliance	
	CM-11	User-Installed Software	
	CM-11(2)	Software Installation with Privileged Status	
	CP-9	System Backup	--
	CP-9(1)	Testing for Reliability and Integrity	--
	CP-9(2)	Test Restoration Using Sampling	--
	CP-9(3)	Separate Storage for Critical Information	--
	CP-9(5)	Transfer to Alternate Storage Site	--

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	CP-9(8)	Cryptographic Protection	
	CP-10(2)	Transaction Recovery	--
	IA-5(13)	Expiration of Cached Authenticators	
	IA-5(14)	Managing Content of PKI Trust Stores	
	IR-4(4)	Information Correlation	
	IR-4(7)	Insider Threats — Intra-Organization Coordination	
	IR-4(8)	Correlation with External Organizations	
	IR-4(11)	Integrated Incident Response Team	
	IR-4(14)	Security Operations Center	
	IR-6(1)	Automated Reporting	
	IR-6(3)	Supply Chain Coordination	
	IR-7	Incident Response Assistance	
	IR-7(1)	Automation Support for Availability of Information and Support	
	IR-7(2)	Coordination with External Providers	
	IR-9	Information Spillage Response	
	IR-9(3)	Post-Spill Operations	
	IR-9(4)	Exposure to Unauthorized Personnel	
	PL-9	Central Management	
	RA-5(10)	Correlate Scanning Information	
	RA-5(11)	Public Disclosure Program	
	SA-4(7)	NIAP-Approved Protection Profiles	
	SA-8(20)	Secure Metadata Management	
	SA-8(28)	Acceptable Security	
	SA-9(1)	Risk Assessments and Organizational Approvals	
	SC-7(12)	Host-Based Protection	
	SC-17	Public Key Infrastructure Certificates	
	SC-18	Mobile Code	
	SC-18(1)	Identify Unacceptable Code and Take Corrective Actions	
	SC-18(2)	Acquisition, Development, and Use	
	SC-18(3)	Prevent Downloading and Execution	
	SC-18(4)	Prevent Automatic Execution	
	SC-23(5)	Allowed Certificate Authorities	
	SI-5	Security Alerts, Advisories, and Directives	
	SI-5(1)	Automated Alerts and Advisories	
	SI-6(3)	Report Verification Results	
	SI-8	Spam Protection	--
	SI-8(2)	Automatic Updates	--

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	SI-12(3)	Information Disposal	
	SR-8	Notification Agreements	
SPACE ENVIRONMENT	AC-5	Separation of Duties	
	AC-11	Device Lock	
	AC-11(1)	Pattern-Hiding Displays	--
	AC-19	Access Control for Mobile Devices	--
	AU-10	Non-Repudiation	
	CA-8(3)	Facility Penetration Testing	
	CM-2(7)	Configure Systems and Components for High-Risk Areas	
	CP-6	Alternate Storage Site	--
	CP-6(1)	Separation from Primary Site	--
	CP-6(2)	Recovery Time and Recovery Point Objectives	--
	CP-6(3)	Accessibility	--
	CP-7	Alternate Processing Site	
	CP-7(1)	Separation from Primary Site	
	CP-7(2)	Accessibility	
	CP-7(3)	Priority of Service	
	CP-7(4)	Preparation for Use	
	CP-8	Telecommunications Services	
	CP-8(1)	Priority of Service Provisions	
	CP-8(2)	Single Points of Failure	
	CP-8(3)	Separation of Primary and Alternate Providers	
	CP-8(4)	Provider Contingency Plan	
	CP-8(5)	Alternate Telecommunication Service Testing	
	IA-6	Authenticator Feedback	
	MP-3	Media Marking	--
	MP-4	Media Storage	--
	MP-5	Media Transport	--
	PE-2	Physical Access Authorizations	--
	PE-3	Physical Access Control	--
	PE-3(1)	System Access	--
	PE-4	Access Control for Transmission	--
	PE-12	Emergency Lighting	--
	PE-13	Fire Protection	--
	PE-13(1)	Detection Systems — Automatic Activation and Notification	--
	PE-13(2)	Suppression Systems — Automatic Activation and Notification	--
	PE-13(4)	Inspections	--

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	PE-15	Water Damage Protection	--
	PE-15(1)	Automation Support	
	PE-16	Delivery and Removal	--
	PE-17	Alternate Work Site	--
	PE-22	Component Marking	
	PE-23	Facility Location	
	SA-9(8)	Processing and Storage Location - U.S. Jurisdiction	
UNCREWED	AC-17(9)	Disconnect or Disable Access	
	IA-12(2)	Identity Evidence	
	IA-12(3)	Identity Evidence Validation and Verification	
	IA-12(4)	In-Person Validation and Verification	
	PS-1	Policy and Procedures	
	PS-2	Position Risk Designation	
	PS-3	Personnel Screening	
	PS-3(4)	Citizenship Requirements	
	PS-4	Personnel Termination	
	PS-4(1)	Post-Employment Requirements	
	PS-4(2)	Automated Actions	
	PS-5	Personnel Transfer	
	PS-6	Access Agreements	
	PS-6(3)	Post-Employment Requirements	
	PS-7	External Personnel Security	
	PS-8	Personnel Sanctions	
	PS-9	Position Descriptions	
	SA-21	Developer Screening	
	SI-4(19)	Risk for Individuals	
USER TRAINING	AT-1	Policy and Procedures	
	AT-2	Literacy Training and Awareness	
	AT-2(2)	Insider Threat	
	AT-2(3)	Social Engineering and Mining	
	AT-2(4)	Suspicious Communications and Anomalous System Behavior	
	AT-2(5)	Advanced Persistent Threat	
	AT-2(6)	Cyber Threat Environment	
	AT-3	Role-Based Training	
	AT-3(1)	Environmental Controls	
	AT-3(2)	Physical Security Controls	--
	AT-4	Training Records	

Vulnerability Assumption	Control	Title	Prev. Space Overlay
	AT-6	Training Feedback	
	CP-3	Contingency Training	
	CP-3(1)	Simulated Events	
	IR-2	Incident Response Training	
	IR-2(1)	Simulated Events	
	IR-2(2)	Automated Training Environments	
	IR-9(2)	Training	
	PL-4	Rules of Behavior	
	PL-4(1)	Social Media and External Site/Application Usage Restrictions	
	SA-8(32)	Sufficient Documentation	
	SA-16	Developer-Provided Training	
	SR-11(1)	Anti-Counterfeit Training	

Appendix B – Controls Added from Threats

Table 5 shows the controls added by threat information informed by SPARTA. For more information on each NIST SP 800-53 control's relationship to SPARTA countermeasures and techniques, a link is provided to the website. There is an additional column "Prev. Space Overlay" to show the previous CNSSI 1253 Attachment 2 to Appendix F, Space Platform Overlay, applied to the CNSSI 1253 dated March 27, 2014. In the overlay column, a "--" identified a control generally not applicable to a H/H/H baseline, while a "+" was for a control generally applicable to be added to a L/L/L baseline.

Table 5 - Controls Added from Threats

ID	Title	Prev. Space Overlay	SPARTA Reference
AC-3(2)	Dual Authorization		https://sparta.aerospace.org/countermeasures/references/AC-3/2
AC-3(3)	Mandatory Access Control		https://sparta.aerospace.org/countermeasures/references/AC-3/3
AC-3(8)	Revocation of Access Authorizations		https://sparta.aerospace.org/countermeasures/references/AC-3/8
AC-3(10)	Audited Override of Access Control Mechanisms		https://sparta.aerospace.org/countermeasures/references/AC-3/10
AC-3(11)	Restrict Access to Specific Information Types		https://sparta.aerospace.org/countermeasures/references/AC-3/11
AC-3(13)	Attribute-Based Access Control		https://sparta.aerospace.org/countermeasures/references/AC-3/13
AC-4(2)	Processing Domains		https://sparta.aerospace.org/countermeasures/references/AC-4/2
AC-4(14)	Security or Privacy Policy Filter Constraints		https://sparta.aerospace.org/countermeasures/references/AC-4/14
AC-25	Reference Monitor		https://sparta.aerospace.org/countermeasures/references/AC-25
AU-5(5)	Alternate Audit Logging Capability		https://sparta.aerospace.org/countermeasures/references/AU-5/5
CA-3(7)	Transitive Information Exchanges		https://sparta.aerospace.org/countermeasures/references/CA-3/7
CP-2(6)	Alternate Processing and Storage Sites		https://sparta.aerospace.org/countermeasures/references/CP-2/6
CP-2(7)	Coordinate with External Service Providers		https://sparta.aerospace.org/countermeasures/references/CP-2/7
CP-4(4)	Full Recovery and Reconstitution		https://sparta.aerospace.org/countermeasures/references/CP-4/4
CP-4(5)	Self-Challenge		https://sparta.aerospace.org/countermeasures/references/CP-4/5
CP-12	Safe Mode		https://sparta.aerospace.org/countermeasures/references/CP-12
CP-13	Alternative Security Mechanisms		https://sparta.aerospace.org/countermeasures/references/CP-13

ID	Title	Prev. Space Overlay	SPARTA Reference
PE-6(2)	Automated Intrusion Recognition and Responses		https://sparta.aerospace.org/countermeasures/references/PE-6/2
PE-19	Information Leakage		https://sparta.aerospace.org/countermeasures/references/PE-19
PE-19(1)	National Emissions Policies and Procedures		https://sparta.aerospace.org/countermeasures/references/PE-19/1
PE-20	Asset Monitoring and Tracking		https://sparta.aerospace.org/countermeasures/references/PE-20
PE-21	Electromagnetic Pulse Protection		https://sparta.aerospace.org/countermeasures/references/PE-21
PM-1	Information Security Program Plan		https://sparta.aerospace.org/countermeasures/references/PM-1
PM-11	Mission and Business Process Definition		https://sparta.aerospace.org/countermeasures/references/PM-11
PM-12	Insider Threat Program		https://sparta.aerospace.org/countermeasures/references/PM-12
PM-14	Testing, Training, and Monitoring		https://sparta.aerospace.org/countermeasures/references/PM-14
PM-16	Threat Awareness Program		https://sparta.aerospace.org/countermeasures/references/PM-16
PM-16(1)	Automated Means for Sharing Threat Intelligence		https://sparta.aerospace.org/countermeasures/references/PM-16/1
PM-17	Protecting Controlled Unclassified Information on External Systems		https://sparta.aerospace.org/countermeasures/references/PM-17
PM-30	Supply Chain Risk Management Strategy		https://sparta.aerospace.org/countermeasures/references/PM-30
PM-30(1)	Suppliers of Critical or Mission-Essential Items		https://sparta.aerospace.org/countermeasures/references/PM-30/1
PM-31	Continuous Monitoring Strategy		https://sparta.aerospace.org/countermeasures/references/PM-31
PM-32	Purposing		https://sparta.aerospace.org/countermeasures/references/PM-32
RA-3(4)	Predictive Cyber Analytics		https://sparta.aerospace.org/countermeasures/references/RA-3/4
RA-5(3)	Breadth and Depth of Coverage		https://sparta.aerospace.org/countermeasures/references/RA-5/3
RA-6	Technical Surveillance Countermeasures Survey		https://sparta.aerospace.org/countermeasures/references/RA-6
SA-4(12)	Data Ownership		https://sparta.aerospace.org/countermeasures/references/SA-4/12
SA-9(6)	Organization-Controlled Cryptographic Keys		https://sparta.aerospace.org/countermeasures/references/SA-9/6
SA-10(2)	Alternative Configuration Management Processes	+	https://sparta.aerospace.org/countermeasures/references/SA-10/2
SA-10(4)	Trusted Generation		https://sparta.aerospace.org/countermeasures/references/SA-10/4
SA-10(5)	Mapping Integrity for Version Control		https://sparta.aerospace.org/countermeasures/references/SA-10/5
SA-10(6)	Trusted Distribution		https://sparta.aerospace.org/countermeasures/references/SA-10/6
SA-11(3)	Independent Verification of Assessment Plans and Evidence	+	https://sparta.aerospace.org/countermeasures/references/SA-11/3

ID	Title	Prev. Space Overlay	SPARTA Reference
SA-11(4)	Manual Code Reviews		https://sparta.aerospace.org/countermeasures/references/SA-11/4
SA-11(5)	Penetration Testing		https://sparta.aerospace.org/countermeasures/references/SA-11/5
SA-11(6)	Attack Surface Reviews		https://sparta.aerospace.org/countermeasures/references/SA-11/6
SA-11(7)	Verify Scope of Testing and Evaluation		https://sparta.aerospace.org/countermeasures/references/SA-11/7
SA-11(8)	Dynamic Code Analysis		https://sparta.aerospace.org/countermeasures/references/SA-11/8
SA-11(9)	Interactive Application Security Testing		https://sparta.aerospace.org/countermeasures/references/SA-11/9
SA-15(5)	Attack Surface Reduction		https://sparta.aerospace.org/countermeasures/references/SA-15/5
SA-15(8)	Reuse of Threat and Vulnerability Information		https://sparta.aerospace.org/countermeasures/references/SA-15/8
SA-17(7)	Structure for Least Privilege		https://sparta.aerospace.org/countermeasures/references/SA-17/7
SC-2(2)	Disassociability		https://sparta.aerospace.org/countermeasures/references/SC-2/2
SC-3(4)	Module Coupling and Cohesiveness	+	https://sparta.aerospace.org/countermeasures/references/SC-3/4
SC-6	Resource Availability	+	https://sparta.aerospace.org/countermeasures/references/SC-6
SC-7(20)	Dynamic Isolation and Segregation		https://sparta.aerospace.org/countermeasures/references/SC-7/20
SC-8(3)	Cryptographic Protection for Message Externals		https://sparta.aerospace.org/countermeasures/references/SC-8/3
SC-8(4)	Conceal or Randomize Communications		https://sparta.aerospace.org/countermeasures/references/SC-8/4
SC-12(3)	Asymmetric Keys	+	https://sparta.aerospace.org/countermeasures/references/SC-12/3
SC-30	Concealment and Misdirection		https://sparta.aerospace.org/countermeasures/references/SC-30
SC-30(5)	Concealment of System Components		https://sparta.aerospace.org/countermeasures/references/SC-30/5
SC-32	System Partitioning		https://sparta.aerospace.org/countermeasures/references/SC-32
SC-32(1)	Separate Physical Domains for Privileged Functions		https://sparta.aerospace.org/countermeasures/references/SC-32/1
SC-40	Wireless Link Protection		https://sparta.aerospace.org/countermeasures/references/SC-40
SC-40(1)	Electromagnetic Interference		https://sparta.aerospace.org/countermeasures/references/SC-40/1
SC-40(3)	Imitative or Manipulative Communications Deception		https://sparta.aerospace.org/countermeasures/references/SC-40/3
SC-40(4)	Signal Parameter Identification		https://sparta.aerospace.org/countermeasures/references/SC-40/4
SC-45(2)	Secondary Authoritative Time Source		https://sparta.aerospace.org/countermeasures/references/SC-45/2
SC-51	Hardware-Based Protection		https://sparta.aerospace.org/countermeasures/references/SC-51

ID	Title	Prev. Space Overlay	SPARTA Reference
SI-3(8)	Detect Unauthorized Commands		https://sparta.aerospace.org/countermeasures/references/SI-3/8
SI-4(7)	Automated Response to Suspicious Events	--	https://sparta.aerospace.org/countermeasures/references/SI-4/7
SI-4(13)	Analyze Traffic and Event Patterns		https://sparta.aerospace.org/countermeasures/references/SI-4/13
SI-7(6)	Cryptographic Protection		https://sparta.aerospace.org/countermeasures/references/SI-7/6
SI-7(12)	Integrity Verification		https://sparta.aerospace.org/countermeasures/references/SI-7/12
SI-13	Predictable Failure Prevention	+	https://sparta.aerospace.org/countermeasures/references/SI-13
SI-13(4)	Standby Component Installation and Notification	+	https://sparta.aerospace.org/countermeasures/references/SI-13/4
SI-14	Non-Persistence		https://sparta.aerospace.org/countermeasures/references/SI-14
SI-14(1)	Refresh from Trusted Sources		https://sparta.aerospace.org/countermeasures/references/SI-14/1
SI-14(3)	Non-Persistent Connectivity		https://sparta.aerospace.org/countermeasures/references/SI-14/3
SI-17	Fail-Safe Procedures		https://sparta.aerospace.org/countermeasures/references/SI-17
SR-4(1)	Identity		https://sparta.aerospace.org/countermeasures/references/SR-4/1
SR-4(2)	Track and Trace		https://sparta.aerospace.org/countermeasures/references/SR-4/2
SR-4(3)	Validate as Genuine and Not Altered		https://sparta.aerospace.org/countermeasures/references/SR-4/3
SR-4(4)	Supply Chain Integrity — Pedigree		https://sparta.aerospace.org/countermeasures/references/SR-4/4
SR-11(3)	Anti-Counterfeit Scanning		https://sparta.aerospace.org/countermeasures/references/SR-11/3

Appendix C – Notional Maximum Tailored Baseline Overlay

Table 6 shows the traditional overlay approach that described all controls that should be added to or removed from a CNSSI 1253 H/H/H baseline to accomplish a space segment notional maximum tailored control baseline. In the overlay column, a “--" is used for a control generally not applicable to a H/H/H baseline, while a “+” is used for a control generally applicable to space segment based on applicable threats.

Table 6 - Notional Maximum Tailored Baseline Overlay

Control	Overlay	Control	Overlay	Control	Overlay	Control	Overlay	Control	Overlay	Control	Overlay
AC-2	--	AC-6(1)	--	AC-18(5)	--	AU-6(3)	--	CM-6(1)	--	CP-8(1)	--
AC-2(1)	--	AC-6(2)	--	AC-19	--	AU-6(5)	--	CM-6(2)	--	CP-8(2)	--
AC-2(2)	--	AC-6(3)	--	AC-19(5)	--	AU-6(6)	--	CM-7(3)	--	CP-8(3)	--
AC-2(3)	--	AC-6(5)	--	AC-20(2)	--	AU-7	--	CM-11	--	CP-8(4)	--
AC-2(4)	--	AC-6(7)	--	AC-21	--	AU-7(1)	--	CM-11(2)	--	CP-8(5)	--
AC-2(5)	--	AC-6(8)	--	AC-22	--	AU-9(4)	--	CP-2(6)	+	CP-9	--
AC-2(7)	--	AC-6(10)	--	AC-23	--	AU-9(6)	--	CP-2(7)	+	CP-9(1)	--
AC-2(9)	--	AC-7	--	AC-25	+	AU-10	--	CP-3	--	CP-9(2)	--
AC-2(11)	--	AC-8	--	AT-1	--	AU-11	--	CP-3(1)	--	CP-9(3)	--
AC-2(12)	--	AC-10	--	AT-2	--	AU-11(1)	--	CP-4(4)	+	CP-9(5)	--
AC-2(13)	--	AC-11	--	AT-2(2)	--	AU-12(1)	--	CP-4(5)	+	CP-9(8)	--
AC-3(2)	+	AC-11(1)	--	AT-2(3)	--	AU-14	--	CP-6	--	CP-10(2)	--
AC-3(3)	+	AC-16	--	AT-2(4)	--	AU-14(1)	--	CP-6(1)	--	CP-12	+
AC-3(8)	+	AC-16(6)	--	AT-2(5)	--	AU-14(3)	--	CP-6(2)	--	CP-13	+
AC-3(10)	+	AC-16(7)	--	AT-2(6)	--	AU-16	--	CP-6(3)	--	IA-2	--
AC-3(11)	+	AC-17(3)	--	AT-3	--	AU-16(1)	--	CP-7	--	IA-2(1)	--
AC-3(13)	+	AC-17(9)	--	AT-3(1)	--	AU-16(2)	--	CP-7(1)	--	IA-2(2)	--
AC-4(2)	+	AC-18	--	AT-3(2)	--	CA-3(7)	+	CP-7(2)	--	IA-2(5)	--
AC-4(4)	--	AC-18(1)	--	AT-4	--	CA-8(3)	--	CP-7(3)	--	IA-2(6)	--
AC-4(14)	+	AC-18(3)	--	AT-6	--	CM-2(3)	--	CP-7(4)	--	IA-2(8)	--

AC-5	--	AC-18(4)	--	AU-5(5)	+	CM-2(7)	--	CP-8	--	IA-2(12)	--
IA-4(4)	--	IR-7	--	MP-2	--	PE-19(1)	+	PS-6(3)	--	SA-11(6)	+
IA-5(1)	--	IR-7(1)	--	MP-3	--	PE-20	+	PS-7	--	SA-11(7)	+
IA-5(2)	--	IR-7(2)	--	MP-4	--	PE-21	+	PS-8	--	SA-11(8)	+
IA-5(8)	--	IR-9	--	MP-5	--	PE-22	--	PS-9	--	SA-11(9)	+
IA-5(13)	--	IR-9(2)	--	MP-6	--	PE-23	--	RA-3(4)	+	SA-15(5)	+
IA-5(14)	--	IR-9(3)	--	MP-6(1)	--	PL-4	--	RA-5(3)	+	SA-15(8)	+
IA-5(16)	--	IR-9(4)	--	MP-6(2)	--	PL-4(1)	--	RA-5(10)	--	SA-16	--
IA-6	--	MA-1	--	MP-6(3)	--	PL-9	--	RA-5(11)	--	SA-17(7)	+
IA-8	--	MA-2	--	MP-7	--	PM-1	+	RA-6	+	SA-21	--
IA-8(1)	--	MA-2(2)	--	PE-2	--	PM-11	+	SA-3(3)	--	SA-22	--
IA-8(2)	--	MA-3	--	PE-3	--	PM-12	+	SA-4(7)	--	SC-2(2)	+
IA-8(4)	--	MA-3(1)	--	PE-3(1)	--	PM-14	+	SA-4(10)	--	SC-3(4)	+
IA-11	--	MA-3(2)	--	PE-4	--	PM-16	+	SA-4(12)	+	SC-6	+
IA-12	--	MA-3(3)	--	PE-5	--	PM-16(1)	+	SA-8(17)	--	SC-7(3)	--
IA-12(1)	--	MA-3(4)	--	PE-6(2)	+	PM-17	+	SA-8(20)	--	SC-7(4)	--
IA-12(2)	--	MA-3(5)	--	PE-8	--	PM-30	+	SA-8(27)	--	SC-7(7)	--
IA-12(3)	--	MA-3(6)	--	PE-8(1)	--	PM-30(1)	+	SA-8(28)	--	SC-7(8)	--
IA-12(4)	--	MA-4	--	PE-8(3)	--	PM-31	+	SA-8(32)	--	SC-7(12)	--
IR-2	--	MA-4(1)	--	PE-12	--	PM-32	+	SA-9(1)	--	SC-7(15)	--
IR-2(1)	--	MA-4(3)	--	PE-13	--	PS-1	--	SA-9(6)	+	SC-7(20)	+
IR-2(2)	--	MA-4(4)	--	PE-13(1)	--	PS-2	--	SA-9(8)	--	SC-7(25)	--
IR-4(4)	--	MA-4(6)	--	PE-13(2)	--	PS-3	--	SA-10(2)	+	SC-7(28)	--
IR-4(7)	--	MA-4(7)	--	PE-13(4)	--	PS-3(4)	--	SA-10(4)	+	SC-8(3)	+
IR-4(8)	--	MA-5	--	PE-15	--	PS-4	--	SA-10(5)	+	SC-8(4)	+
IR-4(11)	--	MA-5(1)	--	PE-15(1)	--	PS-4(1)	--	SA-10(6)	+	SC-12(3)	+
IR-4(14)	--	MA-6	--	PE-16	--	PS-4(2)	--	SA-11(3)	+	SC-15	--
IR-6(1)	--	MA-6(1)	--	PE-17	--	PS-5	--	SA-11(4)	+	SC-17	--

IR-6(3)	--	MP-1	--	PE-19	+	PS-6	--	SA-11(5)	+	SC-18	--
SC-18(1)	--	SI-4(20)	--								
SC-18(2)	--	SI-4(22)	--								
SC-18(3)	--	SI-4(23)	--								
SC-18(4)	--	SI-5	--								
SC-20	--	SI-5(1)	--								
SC-21	--	SI-6(3)	--								
SC-22	--	SI-7(6)	+								
SC-23(5)	--	SI-7(12)	+								
SC-30	+	SI-8	--								
SC-30(5)	+	SI-8(2)	--								
SC-32	+	SI-12(3)	--								
SC-32(1)	+	SI-13	+								
SC-40	+	SI-13(4)	+								
SC-40(1)	+	SI-14	+								
SC-40(3)	+	SI-14(1)	+								
SC-40(4)	+	SI-14(3)	+								
SC-45(2)	+	SI-15	--								
SC-51	+	SI-17	+								
SI-2(2)	--	SR-4(1)	+								
SI-2(3)	--	SR-4(2)	+								
SI-2(4)	--	SR-4(3)	+								
SI-3(8)	+	SR-4(4)	+								
SI-4(7)	+	SR-8	--								
SI-4(13)	+	SR-11(1)	--								
SI-4(14)	--	SR-11(2)	--								
SI-4(15)	--	SR-11(3)	+								
SI-4(19)	--										

Appendix D – Notional Minimum Tailored Baseline Techniques

Table 7 captures all SPARTA red notional risk scores greater than 20 under medium criticality. This correlates with the NSS space segment notional minimum tailored control baseline with high risk tolerance.

Table 7 - Notional Minimum Tailored Baseline Techniques

Technique	Title	Risk Score
IA-0004	Secondary/Backup Communication Channel	24
IA-0004.01	Ground Station	24
IA-0007.02	Malicious Commanding via Valid GS	24
IA-0008	Rogue External Entity	24
IA-0008.01	Rogue Ground Station	24
EX-0001	Replay	24
EX-0001.01	Command Packets	24
EX-0005	Exploit Hardware/Firmware Corruption	24
EX-0005.02	Malicious Use of Hardware Commands	24
EX-0009.01	Flight Software	24
EX-0009.03	Known Vulnerability (COTS/FOSS)	24
EX-0013	Flooding	24
EX-0013.01	Valid Commands	24
EX-0013.02	Erroneous Input	24
EX-0016	Jamming	24
EX-0016.03	Position, Navigation, and Timing (PNT)	24
EX-0014	Spoofing	24
EX-0014.01	Time Spoof	24
EX-0014.02	Bus Traffic	24
EX-0014.04	Position, Navigation, and Timing (PNT)	24
PER-0003	Ground System Presence	24
DE-0002.02	Jam Link Signal	24
EXF-0007	Compromised Ground System	24
REC-0005.01	Uplink Intercept	22
REC-0005.02	Downlink Intercept	22
EXF-0003	Eavesdropping	22
EXF-0003.01	Uplink Intercept	22
EXF-0003.02	Downlink Intercept	22
REC-0001.03	Cryptographic Algorithms	21
REC-0003.04	Valid Credentials	21
IA-0001.03	Hardware Supply Chain	21

Technique	Title	Risk Score
IA-0004.02	Receiver	21
IA-0007	Compromise Ground System	21
IA-0007.01	Compromise On-Orbit Update	21
IA-0010	Exploit Reduced Protections During Safe-Mode	21
EX-0005.01	Design Flaws	21
EX-0006	Disable/Bypass Encryption	21
EX-0009	Exploit Code Flaws	21
EX-0010.03	Rootkit	21
EX-0010.04	Bootkit	21
EX-0011	Exploit Reduced Protections During Safe-Mode	21
EX-0012.03	Memory Write/Loads	21
EX-0012.06	Science/Payload Data	21
EX-0012.08	Attitude Determination & Control Subsystem	21
EX-0012.10	Command & Data Handling Subsystem	21
EX-0012.11	Watchdog Timer (WDT)	21
EX-0016.01	Uplink Jamming	21
PER-0002	Backdoor	21
PER-0002.01	Hardware	21
PER-0002.02	Software	21
PER-0005	Valid Credentials	21
DE-0001	Disable Fault Management	21
DE-0007	Rootkit	21
DE-0008	Bootkit	21
DE-0011	Valid Credentials	21
LM-0001	Hosted Payload	21
LM-0002	Exploit Lack of Bus Segregation	21
LM-0007	Valid Credentials	21
EXF-0008	Compromised Developer Site	21
EXF-0009	Compromised Partner Site	21

Appendix E – Notional Minimum Tailored Baseline Countermeasures

Table 8 captures all unique SPARTA countermeasures associated with the techniques listed in Appendix D and with the removal of noted countermeasures in Table 3.

Table 8 - Notional Minimum Tailored Baseline Countermeasures

Countermeasure	Title
CM0002	COMSEC
CM0006	Cloaking Safe-mode
CM0007	Software Version Numbers
CM0008	Security Testing Results
CM0009	Threat Intelligence Program
CM0010	Update Software
CM0011	Vulnerability Scanning
CM0012	Software Bill of Materials
CM0013	Dependency Confusion
CM0014	Secure boot
CM0015	Software Source Control
CM0016	CWE List
CM0017	Coding Standard
CM0018	Dynamic Analysis
CM0019	Static Analysis
CM0020	Threat modeling
CM0021	Software Digital Signature
CM0022	Criticality Analysis
CM0023	Configuration Management
CM0024	Anti-counterfeit Hardware
CM0025	Supplier Review
CM0026	Original Component Manufacturer
CM0027	ASIC/FPGA Manufacturing
CM0028	Tamper Protection
CM0029	TRANSEC
CM0030	Crypto Key Management
CM0031	Authentication
CM0032	On-board Intrusion Detection & Prevention
CM0033	Relay Protection
CM0034	Monitor Critical Telemetry Points
CM0035	Protect Authenticators

Countermeasure	Title
CM0036	Session Termination
CM0038	Segmentation
CM0039	Least Privilege
CM0040	Shared Resource Leakage
CM0042	Robust Fault Management
CM0043	Backdoor Commands
CM0044	Cyber-safe Mode
CM0047	Operating System Security
CM0048	Resilient Position, Navigation, and Timing
CM0052	Insider Threat Protection
CM0053	Physical Security Controls
CM0054	Two-Person Rule
CM0073	Traffic Flow Analysis Defense
CM0077	Space Domain Awareness
CM0078	Space-Based Radio Frequency Mapping
CM0079	Maneuverability
CM0081	Defensive Jamming and Spoofing
CM0083	Antenna Nulling and Adaptive Filtering

Appendix F – Notional Minimum Tailored Baseline Controls

Table 9 shows the notional minimum set of controls necessary for an NSS space segment per the analysis performed in Section 4.1.

Table 9 - Notional Minimum Tailored Baseline Controls

Minimum Controls for NSS										
AC-3(2)	AU-6	CM-7(5)	IA-4(9)	PM-17	SA-8(9)	SA-11(5)	SC-7(20)	SC-40	SI-4(25)	SR-3(2)
AC-3(10)	AU-6(1)	CM-7(8)	IA-5	PM-30	SA-8(10)	SA-11(6)	SC-7(21)	SC-40(1)	SI-6	SR-3(3)
AC-3(11)	AU-6(4)	CM-7(9)	IA-5(7)	PM-30(1)	SA-8(12)	SA-11(8)	SC-7(29)	SC-40(3)	SI-7	SR-4
AC-3(13)	AU-8	CM-8	IA-7	PM-32	SA-8(13)	SA-11(9)	SC-8	SC-40(4)	SI-7(8)	SR-4(1)
AC-4	AU-9	CM-10	IR-4	RA-3	SA-8(14)	SA-15	SC-8(1)	SC-45	SI-7(9)	SR-4(2)
AC-4(2)	AU-9(2)	CM-10(1)	IR-4(3)	RA-3(1)	SA-8(15)	SA-15(3)	SC-8(3)	SC-45(1)	SI-7(12)	SR-4(3)
AC-4(14)	AU-9(3)	CM-14	IR-4(6)	RA-3(2)	SA-8(18)	SA-15(7)	SC-8(4)	SC-45(2)	SI-7(15)	SR-4(4)
AC-6	AU-12	CP-2	IR-4(12)	RA-3(3)	SA-8(21)	SA-15(8)	SC-10	SC-51	SI-7(17)	SR-5
AC-12	CA-3	CP-2(1)	IR-5	RA-3(4)	SA-8(22)	SA-17	SC-12	SI-2	SI-10	SR-5(1)
AC-14	CA-3(6)	CP-2(3)	IR-5(1)	RA-5	SA-8(23)	SA-17(7)	SC-12(1)	SI-2(6)	SI-10(3)	SR-6
AC-17	CA-3(7)	CP-2(5)	PE-6	RA-5(3)	SA-8(24)	SC-2(2)	SC-12(3)	SI-3	SI-10(5)	SR-6(1)
AC-17(1)	CA-7	CP-2(7)	PE-10	RA-6	SA-9	SC-3	SC-13	SI-3(8)	SI-10(6)	SR-7
AC-17(2)	CA-7(6)	CP-2(8)	PE-20	RA-9	SA-9(6)	SC-4	SC-16	SI-4	SI-11	SR-9
AC-17(10)	CA-8	CP-4(5)	PE-21	RA-10	SA-10	SC-5	SC-16(2)	SI-4(1)	SI-13	SR-9(1)
AU-2	CM-2	CP-10	PL-8	SA-2	SA-10(1)	SC-5(3)	SC-16(3)	SI-4(2)	SI-14(3)	SR-10
AU-3	CM-3(2)	CP-10(4)	PL-8(1)	SA-3	SA-10(3)	SC-6	SC-23	SI-4(4)	SI-16	SR-11
AU-3(1)	CM-3(7)	CP-10(6)	PL-8(2)	SA-4(5)	SA-10(4)	SC-7	SC-24	SI-4(5)	SI-17	SR-11(3)
AU-4	CM-3(8)	CP-12	PM-11	SA-4(9)	SA-10(7)	SC-7(5)	SC-28(1)	SI-4(10)	SR-1	
AU-4(1)	CM-4	CP-13	PM-12	SA-5	SA-11	SC-7(9)	SC-28(3)	SI-4(11)	SR-2	
AU-5	CM-4(1)	IA-3	PM-14	SA-8	SA-11(1)	SC-7(10)	SC-32(1)	SI-4(13)	SR-2(1)	
AU-5(2)	CM-5	IA-3(1)	PM-16	SA-8(3)	SA-11(2)	SC-7(11)	SC-38	SI-4(16)	SR-3	
AU-5(5)	CM-7	IA-4	PM-16(1)	SA-8(4)	SA-11(4)	SC-7(18)	SC-39	SI-4(24)	SR-3(1)	

AEROSPACE REPORT NO.
TOR-2023-02161-Rev A

Space Segment Cybersecurity Profile for National Security Systems - Revision A

Cognizant Program Manager Approval:

Jordan C. Feidler, GENERAL MANAGER
DEFENSE STRATEGIC SPACE
DEFENSE SYSTEMS GROUP

Aerospace Corporate Officer Approval:

Jamie Morin, VICE PRESIDENT
DEFENSE SYSTEMS GROUP

Content Concurrence Provided Electronically by:

Paul De naray, PRINCIPAL ENGINEER/SCIENTIST
PENTAGON AND MULTI-DOMAIN
DEFENSE STRATEGIC SPACE
DEFENSE SYSTEMS GROUP

SQ0578