AEROSPACE REPORT NO.
VTR-2026-00702 – REV A

Ground Segment Cyber Defenses and Risk-Based Tiering – Revision A

March 6, 2026

Brandon T Bailey[1], Paul J de Naray[2] (alphabetical)
[1] Information Systems & Cyber Division
[2] Pentagon and Multi-Domain Division

Prepared for:

U.S. Government Office

Authorized by: Civil Systems Group

AI Disclosure Statement: This report was developed with the assistance of generative AI tools that supported technical editor needs such as refining structure, adding clarity, and ensuring consistency of expert-derived content. All technical editor content was validated by subject matter experts. Models used: OpenAI o3-mini-high, Claude 4.5 Sonnet.

Contents

1. Introduction 1
2. Space System Segments 3
3. Defense-in-Depth Framework 4
4. Risk-Based Tiers 6
   - 4.1 Risk Frameworks and Impact-Based Risk 6
   - 4.2 Establishing a Two-Tier Impact Framework 8
   - 4.3 Implementing a Two-Tier Impact Framework: Baseline and Enhanced Countermeasures 9
5. Ground Segment Mission Functional Breakdown 10
   - 5.1 Threat-Informed Functional Mapping to Defense-In-Depth Countermeasures 12
   - 5.2 Criticality Analysis and Enhanced Countermeasures 12
   - 5.3 Recap of Mission Informed Risk Tiering Approach 13
   - 5.4 Operationalizing the Impact-Based Two-Tier Framework 13
6. Conclusion 14

Appendix A: Defense-in-Depth Sub-layer Definitions 15

Appendix B: Baseline and Enhanced Countermeasures 21

Appendix C: Ground Segment Functional Decomposition Details 92

Appendix D: Attack and Defense Analysis of Viasat KA-SAT Event 100

Appendix E: Acronym List 111

Appendix F: Document References 118

Figures

Figure 1 - Mission Informed, Impact and Threat-Based Risk Tiering Concept 2
Figure 2 - Notional Space System Segments 3
Figure 3 - Ground Segment Defense-in-Depth Layers 5
Figure 4 - Ground Segment Mission Functional Breakdown 11
Figure 5 - Ground Segment Functions Attacked During Viasat KA-SAT Event 101

Tables

Table 1 - DiD Sub-layers 15
Table 2 - DiD Sub-layer Countermeasure Tiers 21
Table 3 - Ground Segment Functional Decomposition Details 92
Table 4 - Defined Attack Chains Against Viasat Ground Segment 103
Table 5 - Viasat Attack Identified DiD Sublayer Countermeasures 104

1. Introduction

This report supports recent United States Government direction and a general need for improved space system ground segment cybersecurity guidance across federal and commercial organizations. This Federally Funded Research and Development Center (FFRDC) analysis is intended as an objective set of recommendations that are bolstered by our demonstrated space system cybersecurity knowledge and expertise across the space enterprise. To accomplish efficient explanations of concepts in this report, this analysis assumes readers have moderate to advanced cybersecurity knowledge as a prerequisite.

This report addresses defining and improving a ground segment's cybersecurity posture through two primary contributions. First, it presents a Defense-in-Depth (DiD) framework specifically tailored to a ground segment. This framework translates established cybersecurity principles into mission-focused capabilities by mapping targeted countermeasures to specific ground segment functions. By defining how layered protections should be implemented, the framework helps to ensure that no single breach can readily compromise critical operational capabilities.

Second, the analysis presents an impact-based, risk management approach utilizing risk tiers to strengthen cybersecurity. This approach organizes defensive countermeasures through the ground segment DiD framework, utilizes risk tiers for implementing countermeasures, and provides a ground segment functional breakdown to support prioritization. This analysis works to promote greater consistency and clarity in how cybersecurity can be applied to a ground segment, while also supporting the implementation of mission defense that is resilient to evolving threats.

A final addition to this analysis is an application of the DiD framework concepts to a real-world ground segment attack. Characterized under the Viasat KA-SAT attack that occurred in February 2022, this analysis characterizes how cyber actors utilized attack techniques and how the defensive DiD countermeasures would have been able to stop the described attack.

Overall, this DiD framework's design is described to offer several strategic advantages for ground segments. The framework integrates with existing organizational risk management processes while minimizing additional regulatory burden and promotes consistency across organizations. By standardizing detailed countermeasures, the framework not only can assist in the protection of a ground segment but will also allow commercial ground segment capability providers to support operations under predictable standards. This approach can expedite the adoption of commercial innovations, reinforcing American leadership in commercial space capabilities. Additionally, the framework's flexibility through impact-

based prioritization supports phased implementations that align with organizational resource constraints and budget cycles.

To foreshadow the methodology described in this report and to orient the reader around concepts that will be explained in subsequent sections, we provide Figure 1 as-is and without full context. This figure illustrates how threats to ground segment mission functions are mapped to layered countermeasures and analyzed for criticality, progressing from baseline protections to enhanced defenses based on risk impact.

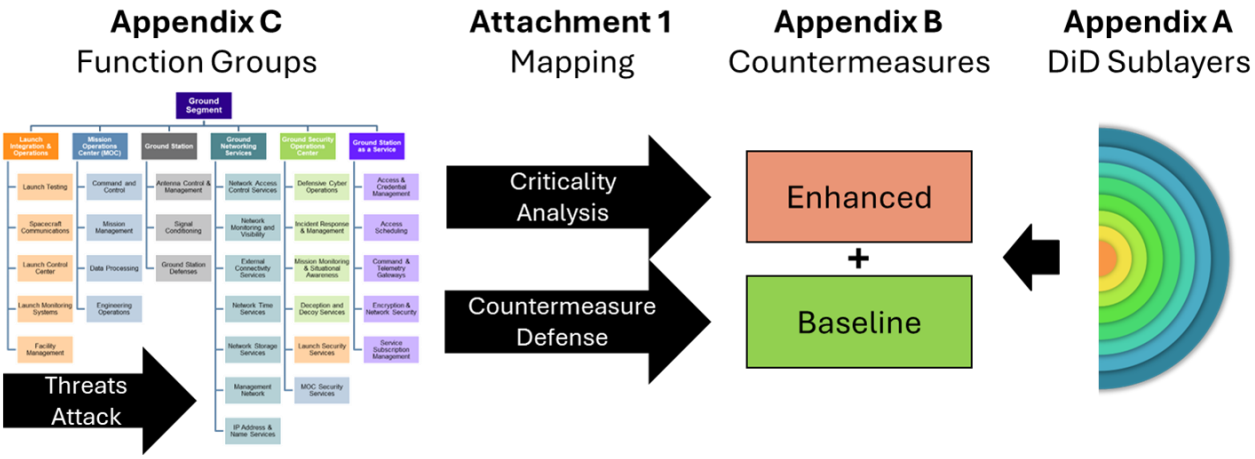

Figure 1 - Mission Informed, Impact and Threat-Based Risk Tiering Concept

2. Space System Segments

A space system is typically defined as having four segments: space, ground, user, and link.

- **Space Segment:** This includes the satellite platform, satellite payloads (e.g., communication, imaging), and onboard computing systems.
- **Ground Segment:** This typically includes the mission operations center, ground stations, ground network infrastructure, software sustainment, and cybersecurity operations. The ground segment also includes aspects for spacecraft integration and launch facilities as those activities occur on the ground in relation to a launch.
- **User Segment:** This includes commodity end-user devices, ground user communication gateways, and custom user applications.
- **Link Segment:** This includes wireless communication within and between the segments. The link segment also includes the components that enable wireless communication (e.g., antennas, transceivers), data encryption, decryption, and transmission security.

This report focuses on the ground segment and the associated link segment components that reside within and support the ground segment. See Figure 2 for a notional depiction of a space system's segments.

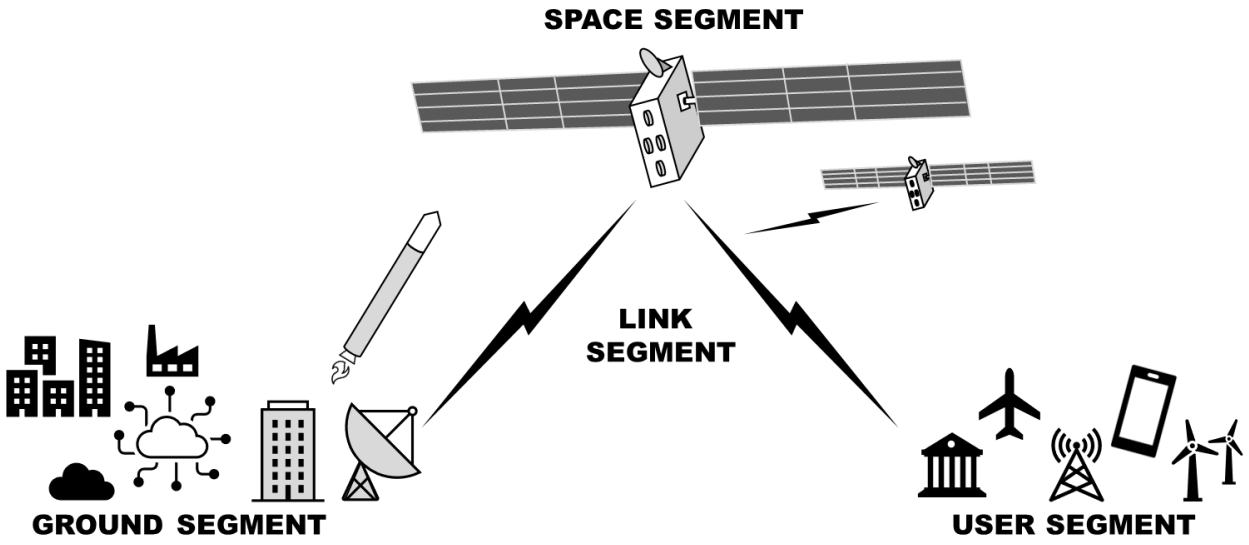

Figure 2 - Notional Space System Segments

3. Defense-in-Depth Framework

A ground segment includes a complex set of functions spread across a system or system of systems. Functions included in a ground segment can also be spread across physical components such as information technology infrastructure, ground antennas, launch vehicle industrial control systems, and networks for commanding and data. Any weak defense in the ground segment can be exploited as an attacker's entry point, from which they can pivot to other parts of the segment. Because no single defensive countermeasure in a system can prevent all adversary tactics, DiD is introduced as a core organizing principle for ground segment cybersecurity.

National Institute of Standards and Technology (NIST) special publication (SP) 800-60 Volume II supports DiD through guidance defining coordinated protection via "Calibrated Defense-In-Depth" to integrate people, technology, and operational capabilities across multiple layers. This layered approach organizes risk-based complementary cyber countermeasures to strengthen overall mission resilience. If one countermeasure fails or is bypassed, additional layers help prevent an adversary from achieving their objectives.

The Aerospace Corporation's work in TOR-2021-01333 Revision A and the subsequent SPARTA framework established precedence for implementing a DiD approach to develop cybersecurity baselines. Space segment layers and sub-layers were first defined; these definitions were then used to identify notional threats and vulnerabilities. These identified threats formed the basis for developing threat tactics and techniques within the SPARTA framework, which in turn were used to create defensive SPARTA countermeasures. This body of countermeasures served as a knowledge base for the Committee on National Security Systems (CNSS) as they tailored cybersecurity controls for space segment defenses in CNSS Instruction 1253. The DiD framework precedence demonstrates an integrated perspective that supports the development of informed and customized cyber countermeasures.

Since the definition of the SPARTA space segment DiD layers, Aerospace also published a notional ground segment DiD framework. Figure 3 depicts eight DiD layers that can define and coordinate protection for a ground segment. The layers represent a logical separation of notional ground segment countermeasures. Identified below are sub-layers for each layer; there are 78 sub-layers identified to depict specific defensive countermeasures. These sub-layers were developed based on subject matter expertise in both notional and existing defensive ground segment capabilities, as well as experience gained from successful red team compromises. Definitions for each sub-layer can be found in Appendix A.

- **Data:** Encryption; Data Loss Prevention – Data; Access Control – Data; Sensitive Data Access Control
- **Ground Software:** Configuration Control - Build Environment; Secure Coding Standards; Common Weakness Enumeration Prevention; Documentation / Diagrams - Software; Dynamic Analysis Testing; Supply Chain Risk Management – Software; Static Analysis Testing; Threat Modeling.
- **Endpoint:** Application Whitelisting; Logging & Auditing; Authentication - Endpoint; Malicious Code Protection; Backups; Configuration Control / Endpoint Baseline; Separation of Duties; Data Loss Prevention - Endpoint; File Integrity; Host Firewall; Hardening - Endpoint; Host-based Intrusion Detection System / Host-based Intrusion Prevention System; Memory Protection; Patch Management; File Permissions; Remote Access; Service Configuration; User Least Privilege; Vulnerability Scanning.

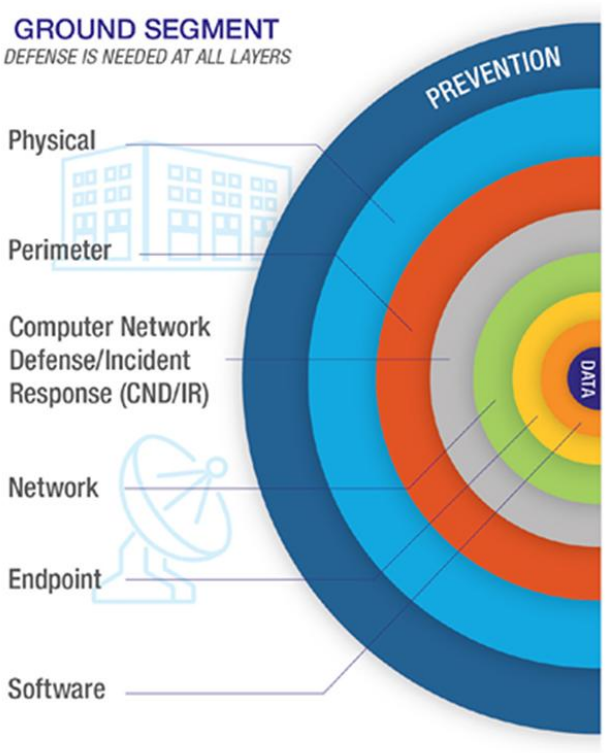

Figure 3 - Ground Segment Defense-in-Depth Layers

- **Network:** Reverse Proxy; Access Control Lists; Authentication - Network Administration; Configuration Management - Network; Hardening - Network Devices; Diversification of Network Paths; Documentation/Diagrams - Network; Internal Firewall; Logging - Network; Network Access Control - Device Authorization; Network Operations Center; Network Time Protocol; Port Security; Segmentation; Simple Network Management Protocol (SNMP); Trunking; Remote Management Access; Web Proxy; Wireless.
- **Computer Network Defense / Incident Response:** Forensics; Hunting; Threat Intelligence; Intrusion Detection / Prevention System; Incident Response Policy / Procedures; Sensors; Security Information & Event Manager; Security Operations Center; Test Access Points.
- **Perimeter:** Web Application Firewall; Virtual Private Network / Remote Access; Data Loss Prevention - Perimeter; Demilitarized Zones / Security Zones; Perimeter Firewall.
- **Physical:** Badging / Doors; Fire Suppression; Gates/Guards; Logging - Physical; Mission Security Personnel; Infrastructure Diversity; Surveillance.
- **Prevention:** Personnel Awareness; Personnel Management; Security Assessments; Threat Assessment; End-user Training; Information Security Staff Training; Supply Chain - Prevention.

For comprehensive defense of a ground segment, all DiD layers should be implemented to some degree; ignoring a layer likely incurs significant mission risk. DiD is a strategic approach that helps to ensure space missions can withstand the inevitable reality of new and unknown cyber threats finding weaknesses to exploit in a ground segment.

4. Risk-Based Tiers

This analysis was focused on identifying risk-based ground segment tiering categories and an associated risk methodology for implementing countermeasures. This risk-based approach would also identify instances where linkages exist to on-orbit systems or other relevant systems and describe categories for proposed risk tiers.

4.1 Risk Frameworks and Impact-Based Risk

There are many risk assessment frameworks that exist within the federal government that define and prescribe approaches to assess risk. For instance, there is the NIST Cybersecurity Framework (CSF) 2.0 that offers a taxonomy of high-level cybersecurity outcomes that can be used by any organization to better understand, assess, prioritize, and communicate cybersecurity efforts. Even further under CSF is an existing NIST Interagency Report (IR) 8401 "Satellite Ground Segment - Applying the Cybersecurity Framework to Satellite Command and Control" that utilizes the CSF to create a profile for the space sector's ground segment. As the CSF and NIST IR 8401 describe positive aspects such as strategic planning, stakeholder communication, and demonstrating recommendations for defensive considerations, we found that this approach will not align with an intended goal of providing risk-based tier guidance with systems security engineering concepts. There is a fundamental mismatch in CSF risk analysis where it is not oriented around a risk-tier approach. CSF is a function-focused breakdown of categories and subcategories to define higher-level defensive outcomes for a system.

A common approach for cybersecurity risk assessment across the federal government is to utilize the NIST SP 800-30 "Guide for Conducting Risk Assessments," with impact and likelihood risk factors. 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 the probability that a threat can exploit a system's specific vulnerability. Within this report's analysis approach, we do not specifically know each ground segment's unique threats and vulnerabilities that can determine specific risk likelihood. For example, a system's vulnerabilities can be specific to the system design and can also be lessened by already deployed defensive countermeasures. In addition, a system's threat sources can be unique based on the adversary's intent and interest in compromising the system.

While there is uncertainty in NIST SP 800-30 risk likelihood, we leverage multiple aspects of impact to serve as a primary risk indicator. The default federal approach to categorizing impact-based risk is the Federal Information Processing Standards Publication (FIPS) 199 framework that defines three levels of potential impact resulting from information compromise. These three levels are low, moderate, and high impact based on determining limited, serious, or severe/catastrophic effects, respectively, when information is compromised. Based on this information impact determination, a program can then utilize the NIST SP 800-37 "Risk Management Framework for Information Systems and Organizations" to categorize systems and determine default protection baselines.

However, while FIPS 199 has become prevalent for assessing impact-based risk around the compromise of information, we propose expanding impact considerations to include other aspects that provide a more holistic impact-based, risk management approach. There are existing methodologies that define other impact aspects, such as the NIST SP 800-39 "Managing Information Security Risk Organization, Mission, and Information System View" for multi-tiered risk management across the organization, mission, and information system, or the NASA SP-20240014019 "Risk Management Handbook" that describes risk management across centers, programs, missions, and technical tasks. These approaches utilize not only technical system and information impact but also the mission purpose consideration and the organization perspectives. The mission purpose is driven by considerations such as the importance of functions being performed and the performance of the system for meeting defined objectives. The organization perspectives drive organizationally calibrated factors such as the system's cost, lifecycle phase, and interconnected exposure to other systems. At a basic level, we present a combination of multiple impact factors to define, understand, and manage ground segment risk across a system lifecycle.

Starting with the more technical aspects of a ground segment, we leverage the standard FIPS 199 information compromise levels of low, moderate, and high to calibrate expected initial impact levels. There is existing federal guidance that provides some consensus insight in relation to space systems information impacts. The NIST SP 800-60 Volume II, "Guide for Mapping Types of Information and Information Systems to Security Categories" describes information types relevant to space missions and supporting ground infrastructure:

- **D.11.4 – Space Operations Information Type**: Involves the activities related to the safe launches/missions of passengers or goods into aerospace and includes commercial, scientific, and military operations. *Security Category = {(confidentiality, Low), (integrity, High), (availability, High)}*

- **D.19.2 – Space Exploration and Innovation Information Type**: Includes all activities devoted to innovations directed at human and robotic space flight and the development and operation of space launch and transportation systems, and the general research and exploration of outer space. *Security Category = {(confidentiality, Low), (integrity, Moderate), (availability, Low)}*

Furthermore, following the approach defined in NIST SP 800-60, Volume I, for "high water mark" system categorization, this can set expectations on system impact. Based on D.19.2's moderate integrity rating, systems supporting a ground segment should be categorized as having at least a moderate level of information impact. Based on D.11.4's high integrity and high availability ratings when safety of life is at stake, systems supporting a ground segment should be categorized as having a high level of information impact. These space-related information types are likely to exist for any ground segment mission, and this would drive an expectation that no system supporting a ground segment would be categorized as a low level of information impact to the ground segment.

4.2 Establishing a Two-Tier Impact Framework

Moving to organizational impact considerations provides context for decisions that drive overall risk management activities across programs. The organization will usually direct internal funding decisions across the enterprise based on many factors, including multiple programs, changing priorities, and external factors. These funding decisions can have a direct impact on how cybersecurity is implemented as those capabilities need resources for development and sustainment. Every organization faces limited cybersecurity budgets, and the available resources will usually be prioritized towards countermeasure implementation in high and moderate risk impact systems. Appropriately, this situation leaves few resources to be allocated for low impact systems. As a result of these resource constraints, a low impact system will likely have less countermeasures and as a result have vulnerabilities available for threat exploitation and system compromise. When the organization accounts for the integrated set of connected systems in a ground segment, this vulnerable, low impact system can now become a pivot point for access to higher impact systems.

A basic countermeasure to handle these low impact system compromises would be to physically isolate (e.g., air gap) the system from the higher impact systems. However, physically isolating low impact systems within a ground segment is often impractical due to modern requirements for interconnected capabilities and the underlying mission need to integrate these systems. If a low impact system must be connected within a ground segment containing higher impact systems, then that low impact system's risk must be directly managed within the overall ground segment. At the very least, there will need to be technical countermeasures implemented across the low impact system's interconnection to the ground segment. With respect to DiD layers, this likely includes countermeasures across the

Computer Network Defense / Incident Response, Network, Endpoints, Ground Software, and Data. These countermeasures will have to be specifically tailored for how this low impact system interfaces and operates with the ground segment to appropriately manage the risk. Optimally, the low impact system would align its countermeasures to match or inherit the same baseline expectations of the higher impact system so there is more uniform protection across the interconnected ground segment. Taken together, this system-of-systems dynamic makes standalone low impact categorizations difficult to justify within an interconnected ground segment and supports the conclusion, derived from NIST SP 800-60 guidance, that ground segments are unlikely to qualify as low impact.

It should be noted that while interconnectedness makes low impact categorization unlikely, it does not mean impact inheritance should be applied indiscriminately across all systems. Carrying this logic too far would cause any single high impact system to make all other systems in the ground segment also have a high impact. Given limited cybersecurity budgets, this approach would be inefficient as it would likely result in the overprotection of moderate impact systems.

Based on information and organizational impact analysis, we establish the expectation that all connected systems in a ground segment will generally be characterized as moderate or high level of information impact. This expectation establishes two system impact-based risk tiers: moderate impact as the baseline, and high impact applied where mission or safety considerations warrant enhanced protection. While limited cases of lower impact system interconnections may exist and require tailored countermeasures, we maintain a baseline expectation for an organization to target protecting a moderate level of information impact across the ground segment.

4.3 Implementing a Two-Tier Impact Framework: Baseline and Enhanced Countermeasures

We next characterize these impact-based risk tiers through mapping DiD sublayer countermeasures to each tier. To perform this mapping, we establish that the moderate information impact tier serves as the baseline for implementing DiD sub-layers. The recommended ‘Baseline’ countermeasures for each DiD sub-layer are defined in Appendix B. This set of recommended countermeasures reflects subject matter expertise informed by significant experience with ground segment assessments to identify vulnerabilities and the countermeasures available to protect systems with current technology. While all DiD layers will likely apply to a system, the Baseline countermeasures are not prescribed such that all DiD sub-layers must be applied. Rather, ground segments have unique characteristics based on mission needs and architecture design choices. The unique design and implementation choices of a system will make some sub-layers apply and others not. The DiD sub-layer countermeasures should be viewed as recommended implementation

configurations and capabilities when that sub-layer is applicable. Further explanation and details about determining appliable DiD sub-layer countermeasures are described in Section 5.

With respect to a tier for high information impact considerations, we define 'Enhanced' DiD sub-layer countermeasures that incorporate more complex and resource-intensive technology to provide additional protection where warranted. These Enhanced countermeasures provide greater assurance and risk reduction beyond the baseline implementation. Each Enhanced countermeasure is only recommended to be selected when necessary and is to be applied in addition to the baseline countermeasure. This selective approach with Enhanced DiD sub-layer countermeasures supports efficient application of the organizational budget to cybersecurity capabilities in the highest impact areas. The rationale for selecting an Enhanced countermeasure is explained further in Section 5. The high impact tier 'Enhanced' DiD sub-layer countermeasures are further defined in Appendix B.

5. Ground Segment Mission Functional Breakdown

To assist with understanding ground segment cyber defenses, we provide a functional breakdown of a ground segment's cyber terrain in Figure 4. This breakdown depicts mission areas and function groups that collectively perform the ground segment mission. This type of orientation helps system security engineers to enumerate and analyze cybersecurity capabilities across the ground segment. These function groups and the functions therein are the foundation for how mission impacts are considered in risk assessment and mitigations.

The main ground segment *mission areas* are Launch Integration and Operations, Mission Operations Center, Ground Station, Ground Networking Services, Ground Security Operations Center, and Ground Station as a Service. While many of these mission areas support the sustained operational phase of a ground segment mission, some areas are limited to a specific mission phase, such as the Launch Integration and Operations that are applied prior to and during spacecraft launch. Each mission area includes the depicted *function groups* that define a logical collection of *functions* supporting the overall mission area. The defined functions must be defended to ensure continued mission execution. The function groups and functions are further defined in Appendix C.

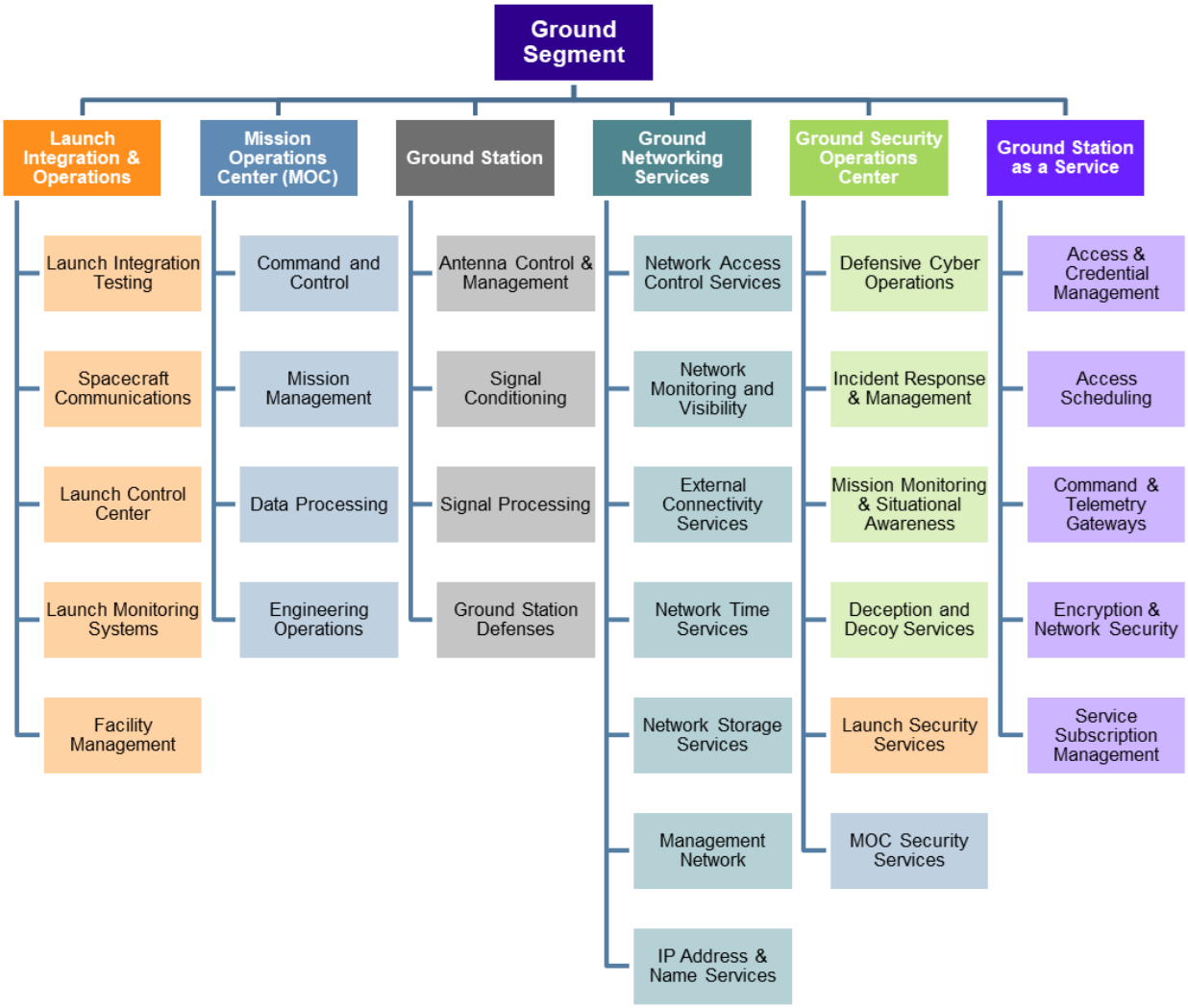

Figure 4 - Ground Segment Mission Functional Breakdown

Not all organizations that own or operate a ground segment will perform every defined mission area, function group, or function. Responsibilities and dependencies vary across missions and organizational models, and functions may be distributed across internal systems or provided by external partners or service providers. For instance, an organization may perform its Mission Operations Conter using its own developed systems while relying on a separate system and organization to perform Launch Integration and Operations.

Within this context of distributed capabilities, there is an aspect to note about the security services shown in Figure 4. Under the Ground Security Operations Center mission area, the security services for Launch and Mission Operations Center are also included. These two security services could reside within the original mission area or they could be consolidated into an integrated ground segment Ground Security Operations Center, as indicated.

5.1 Threat-Informed Functional Mapping to Defense-In-Depth Countermeasures

To effectively design ground segment defenses, system security engineers must understand the deployed set of functions across the ground segment to support the ground mission. A complete system functional breakdown is necessary to understand how the system aligns with the overall mission, organization responsibilities, system architecture, and implemented capabilities. There can be any number of unique missions, designs, and capabilities developed over differing eras, technologies, and organizational choices. An understanding of how mission functions relate to a ground segment directly informs how cybersecurity capabilities are designed and implemented across DiD sub-layers.

To relate the system functional breakdown to the DiD sub-layer countermeasures, we provide a notional mapping between each individual function group and sub-layers in Attachment 1. This mapping product is driven by Aerospace threat-based analysis that first correlated all ground segment function groups with appropriate MITRE ATT&CK techniques. These techniques were matched through applicable attacks against each function, which then provided context to select corresponding DiD sub-layer countermeasures that countered each technique. This mapping process provides actionable insight into how threat techniques can be leveraged against specific ground segment function groups and why particular countermeasures are recommended. Understanding why countermeasures are applied helps in implementing effective measures and avoids unguided application of generic protection technology.

The mapping knowledge provided in Attachment 1 enables systems security engineers to identify which countermeasures apply to which specific function group across the ground segment, therefore enabling targeted implementation. Analysis will need to be performed by engineers to identify the function groups within each system. These function groups then enable the mapping of DiD sub-layer countermeasures with applicable ATT&CK techniques to the specific architecture components in each system. This approach avoids indiscriminate application of a monolithic set of Baseline countermeasures across the entire ground segment.

5.2 Criticality Analysis and Enhanced Countermeasures

The application of Enhanced countermeasures is for those mission functions that must be protected with stronger protections added to the Baseline countermeasure. These Enhanced countermeasures are selected through additional system security engineering that performs criticality analysis against the mission's function groups. The determination of function groups that could have the highest mission impact (i.e., severe/catastrophic) are those that must be traced through Attachment 1 to the possible associated DiD sub-layers. Through this criticality analysis and tracing to DiD sub-layers, system security engineering

can then select applicable Enhanced countermeasures to apply in addition to the Baseline countermeasures. As each ground segment is unique with mission purpose and functional design, criticality analysis must be uniquely performed for each system. This limited application of Enhanced countermeasures should enable an organization to apply limited resources to those DiD sub-layers that will provide the most protection for the most impactful mission function groups.

5.3 Recap of Mission Informed Risk Tiering Approach

To summarize the risk-based tiering approach we point the reader back to the introduction's first illustration in Figure 1. Appendix A defines the structure for all DiD sub-layers, and Appendix B provides separate Baseline and Enhanced countermeasures for each sub-layer. The ground segment mission functional breakdown, defined in Appendix C, provides the operational context for how a system could be attacked through MITRE ATT&CK techniques. In Attachment 1, ground segment function groups are linked to DiD countermeasures through the selection of defenses that mitigate threat techniques. Finally, Enhanced countermeasures are selected through criticality analysis against functional groups and traced to relevant DiD sub-layers.

To further demonstrate how this DiD framework analysis applies to ground segments, we provide an analysis of a real-world cyber attack on a space system ground segment in Appendix D. This analysis demonstrates how ATT&CK techniques are correlated with cyber actor efforts to accomplish significant impact across the space system. However, we also present how DiD countermeasures defined in Appendix B would have been able to stop the cyber actor's attack chain. This analysis helps to explain and justify the purpose of DiD countermeasures to protect a ground segment.

5.4 Operationalizing the Impact-Based Two-Tier Framework

There are many organizational considerations that can be factored into a ground segment across a system lifecycle. Most systems in existence are already in the operations and maintenance phase of a space mission, but some may be in development for an upcoming spacecraft launch or early in the development lifecycle. The earlier a system is in the development lifecycle, the more likely an incorporation of Baseline and Enhanced countermeasures is possible as requirements are being written, and design is occurring. If a system is already in operation, then there can be significant challenges with having resources available for incorporating additional capability and avoiding unnecessary impact on the operational mission.

For any efforts that align systems to the framework described in this report, we first recommend that each system perform a functional decomposition of the architecture in

relation to the ground segment functions or at the very least to function groups. This analysis will create a mapping of necessary countermeasures for each function group, and those countermeasures can be compared against the countermeasures currently implemented in the system. Once systems have assessed their current state of countermeasure implementation, the next step would be to work across organizational resources to determine which additional countermeasures should be implemented. Gaps between current state and target protections will have to be balanced against organizational factors such as costs, mission importance, and remaining mission duration. This effort can also be aligned with the previously defined functional decomposition and criticality analysis to understand the most critical functions to protect.

6. Conclusion

The Aerospace Corporation has developed a Defense-in-Depth framework specifically tailored to protect ground segments that control key U.S. space missions. This framework translates established cybersecurity principles into practical capabilities that directly bolster national resilience. Although DiD is a foundational concept for creating trustworthy systems, this work advances the concept by mapping targeted countermeasures to the mission-critical functions of a ground segment. This approach prioritizes functions that must be protected against adversary attack to ensure uninterrupted mission operations.

Moreover, by defining how layered protections are implemented, the framework ensures that no single breach can readily compromise critical operational capabilities. This framework is designed to integrate with existing organizational risk management processes by enhancing understanding of why specific countermeasures are necessary. This integrated approach will minimize additional regulatory burden and promote consistency across organizations. Standardizing these detailed countermeasures also allows commercial capability providers to support operations under a predictable standard, expediting the adoption of commercial innovations without sacrificing security. Facilitating greater integration of commercial solutions into ground segments will reinforce American leadership in commercial space capabilities. Additionally, the framework's flexibility, through impact-based prioritization, supports phased implementations that align with organizational resource constraints and budget cycles. Overall, deploying this framework offers a practical and actionable strategy to strengthen mission assurance, safeguard critical capabilities, and maintain the resilience of U.S. ground segments in the face of evolving cyber threats.

Appendix A: Defense-in-Depth Sub-layer Definitions

Table 1 provides full definitions for each DiD sub-layers and adds identifications that support further referencing.

Table 1 - DiD Sub-layers

DiD Layer	Layer ID	DiD Sub-Layer	Definition
Data	**DAT-1**	**Encryption**	The use of cryptographic algorithms paired with disciplined key management practices to protect mission-critical data both at rest and in transit. This control ensures not only confidentiality and integrity but also authentication across communications between spacecraft, ground systems, and partners.
	DAT-2	**Data Loss Prevention - Data**	Data loss prevention (DLP) controls avoid accidental or unauthorized exposure of sensitive information such as credentials or mission files. The controls are a combination of policy, monitoring, and technical safeguards to detect and block exfiltration across endpoints, networks, and cloud services.
	DAT-3	**Access Control - Data**	Role-Based Access Control (RBAC) and Attribute-Based Access Control (ABAC) provide methods to control data access. RBAC assigns data access permissions based on a defined user role and enables least privilege enforcement. ABAC also governs access but is based on dynamic entity attributes such as user, resources, actions, or other context conditions.
	DAT-4	**Sensitive Data Access Control**	Sensitive-data access governs mission critical artifacts under stricter controls, such as command/telemetry databases, cryptographic material, and mission plans. The controls add additional authentication, approvals, and auditing to minimize risks, such as insider threats and attacker misuse of file shares or repositories.
Custom Software	**CSW-1**	**Configuration Control - Build Environment**	Process of controlling modifications to software to protect the information system against improper modifications. Build and configuration control creates repeatable and trustworthy software releases. The build environment enforces cryptographic integrity and provenance of software artifacts through controlled access, repeatable builds, and release validation ensuring deployed binaries are derived only from authorized source code, configurations, and approved toolchains.
	CSW-2	**Secure Coding Standards**	Secure coding standards are the codified rules, patterns, and prohibited practices that developers follow to prevent vulnerabilities during design and implementation. These standards include checks for input validation, memory safety, authentication/authorization, crypto use, error handling, logging, and third-party dependencies. Enforcement is built into the workflow via linters, peer review checklists, and continuous integration / continuous deployment (CI/CD) gates, and the standards are updated regularly as threats and tech stacks evolve.
	CSW-3	**Common Weakness Enumeration Prevention**	Common Weakness Enumeration (CWE) prevention targets high-risk software weakness classes relevant to the mission. It prioritizes mitigations and checks that block these flaws from entering the codebase.
	CSW-4	**Documentation/Diagrams - Software**	Architecture documentation and data-flow diagrams describe where the software runs, how components interact, and which data are exchanged. They provide a shared source of truth for engineering, assessment, and incident response.
	CSW-5	**Dynamic Analysis Testing**	The practice of executing software in production-like, high-fidelity environments to reveal runtime vulnerabilities, logic errors, and misconfigurations that static analysis may overlook. This testing supports regression checks, operator training, and the discovery of zero-day issues.
	CSW-6	**Supply Chain Risk Management - Software**	Software supply chain risk management involves the consumption and utilization of software bill of materials (SBOMs) to manage risk from software dependencies across the software development lifecycle. Consumption includes analysis of collected SBOMs for provenance and pedigree of dependencies. Software dependency analysis also includes utilizing SBOMs for enrichment activities supporting risk assessment (e.g., Common Vulnerabilities and Exposures (CVE) identification, foreign influence, secure software development).

	CSW-7	**Static Analysis Testing**	Static analysis inspects source or binaries without executing them to detect vulnerabilities and unsafe patterns early. This testing complements reviews with automated checks aligned to mission coding standards and CWE priorities.
	CSW-8	**Threat Modeling**	Threat modeling identifies likely adversaries, attack paths, and mitigations across the system's design and operations. Threat modeling informs control selection, test planning, and risk prioritization throughout the lifecycle.
Endpoint	**END-1**	**Application Whitelisting**	A security control that only allows a pre-approved set of applications to execute on endpoints. This approach minimizes the risk of malware execution and unauthorized software exploitation.
	END-2	**Logging & Auditing**	Systematic collection, analysis, and review of activity logs and system events on individual endpoints. This capability ensures that an organization can verify that endpoints are operating according to established security policies. Centralized analysis of logging can correlate events and assist in incident detection and response activities.
	END-3	**Authentication - Endpoint**	Verifying the identity of a user, process, or device attempting to access a specific endpoint (e.g., desktops, laptops, servers, or mobile devices). This capability ensures that only authorized entities can gain access to or within endpoint resources. Example aspects include user or process credentials, multi-factor authentication (MFA), integration with endpoint security hardware (e.g., trusted platform module, secure boot), and device authentication.
	END-4	**Malicious Code Protection**	Endpoint defenses to detect and stop malicious software and behavior. This capability can combine signature, behavioral, and sandbox techniques.
	END-5	**Backups**	Backups preserve recoverable copies of endpoint critical systems. Hardened, tested backups enable rapid restoration and resilience during compromises to endpoint integrity.
	END-6	**Configuration Control / Endpoint Baseline**	Process of controlling modifications to hardware, firmware, software, and files to protect the information system against improper modifications. Endpoint baselining sets and enforces secure configurations across devices. Integrity checks also track unauthorized changes to important files.
	END-7	**Separation of Duties**	Separation of duties on endpoints helps to prevent any single user, process, or system entity role from having complete control over critical endpoint operations. By dividing responsibilities across distinct roles, accounts, and/or devices, this capability limits impact from attacks such as credential compromise or insider threat.
	END-8	**Data Loss Prevention - Endpoint**	Endpoint DLP monitors and controls how sensitive data is handled on endpoints. DLP detects risky transfers from the endpoint and prevents inadvertent or malicious data loss.
	END-9	**File Integrity**	File integrity monitoring tracks unauthorized changes to critical files and configurations. Cryptographic hashing and alerting help spot tampering early.
	END-10	**Host Firewall**	Host firewalls exist on endpoints to control inbound and outbound traffic by enforcing policies tailored to the specific device's role and security posture. These capabilities can enforce least-privilege for network access from the endpoint, perform traffic filtering, and block unauthorized traffic.
	END-11	**Hardening - Endpoint**	Endpoint hardening disables unnecessary services and applies secure settings across the endpoint capabilities. Standardized configurations (e.g., Security Technical Implementation Guide (STIG), Center for Internet Security (CIS) benchmark) can reduce attack surfaces. Retained services are hardened through aspects such as minimizing privileges, securing service parameters, and removing default accounts and daemons.
	END-12	**Host-based Intrusion Detection System / Host-based Intrusion Prevention System**	Host-based Intrusion Detection System (HIDS) / Host-based Intrusion Prevention System (HIPS) monitor endpoint behavior and enforce prevention rules on the host. HIDS/HIPS detects suspicious activity and can block or contain attacks locally.
	END-13	**Memory Protection**	Hardware and software-based capabilities to safeguard endpoint memory against unauthorized access, corruption, and exploitation. Controls include Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), exploit guards, and control-flow integrity.
	END-14	**Patch Management**	The systematic notification, identification, deployment, installation, and verification of operating system and application software code revisions. Patch management keeps software up-to-date by rapidly fixing known vulnerabilities.

	END-15	**File Permissions**	File permissions and access controls define which users, services, and processes can read, write, execute, or modify files and directories based on role and operational need. Properly enforced permissions apply least-privilege principles, prevent unauthorized access to mission-critical data and executables, and reduce the risk of accidental or malicious modification. Permissions are managed through explicit ownership, group membership, and access control rules, and are regularly reviewed to ensure alignment with current operational roles and mission phases.
	END-16	**Remote Access**	Controlled processes by which users or systems connect to endpoints. The capabilities leverage secure protocols, multi-factor authentication, encryption, and device integrity verification to ensure that only secure and authorized remote sessions are established.
	END-17	**Service Configuration**	Service configuration ensures background services run with minimal privileges and secure settings. It eliminates default accounts, hardens service parameters, and removes unnecessary daemons.
	END-18	**User Least Privilege**	User least privilege limits access to only what is necessary to perform a required role. This reduces the impact of account compromise and curbs lateral movement.
	END-19	**Vulnerability Scanning**	Automated scanning to identify weaknesses and known vulnerabilities on endpoints. Authenticated, continuous scans feed remediation workflows and risk reporting.
Network	**NET-1**	**Reverse Proxy**	Reverse proxies protect mission servers from direct client connections by acting as a network intermediary for the internal network, accepting incoming client requests and forwarding them to one or more servers. These capabilities support traffic routing, connection termination, IP address concealment, policy enforcement, and integration with other network functions like firewalls and web application firewalls.
	NET-2	**Access Control Lists**	Access Control Lists (ACLs) are rule sets applied to routers, switches, and firewalls that define which traffic is permitted or denied within a ground segment network. The capabilities involve filtering packets based on attributes such as IP address, protocol, or port to enforce policy and segment networks.
	NET-3	**Authentication – Network Administration**	Processes and controls used to verify the identity of administrators who access and manage network infrastructure devices. This capability ensures that only authorized personnel can perform configuration changes, troubleshooting, or maintenance on critical network components. Modern implementations pair strong credentials with multi-factor checks and disable legacy login paths.
	NET-4	**Configuration Management - Network**	Processes for maintaining, monitoring, and controlling the settings and configurations of network infrastructure to ensure consistency and security. This capability is essential for supporting an organization's network integrity and resilience.
	NET-5	**Hardening – Network Devices**	Network device hardening is the process for securing network infrastructure by applying practices, controls, and configurations to reduce vulnerabilities and to minimize attack surfaces. Practices include disables unnecessary services, applying secure settings with standardized secure baselines (e.g., STIGs, CIS benchmarks), access controls, and secure management communication.
	NET-6	**Diversification of Network Paths**	Network path diversification builds resilient, fault-tolerant connectivity. Redundant and geographically diverse links prevent single points of failure.
	NET-7	**Documentation/Diagrams - Network**	Network architecture documentation and data-flow diagrams describe how devices are connected across the system. They provide a shared source of truth for engineering, assessment, and incident response.
	NET-8	**Internal Firewall**	Internal Firewalls enforce security boundaries between different enclaves or zones within the ground segment network. Unlike perimeter firewalls that protect against external threats, these devices or controls focus on segmenting internal mission systems, ensuring that sensitive operations (e.g., command and telemetry, admin functions, user services) are isolated from one another.
	NET-9	**Logging - Network**	Logging on Network Devices and ACLs captures and records security-relevant events such as connection attempts, rule matches, configuration changes, and traffic denials. These logs provide vital visibility into how routers, switches, and firewalls are being used and whether ACLs are functioning as intended.

	NET-10	**Network Access Control - Device Authorization**	Network Access Control (NAC) – Device Authorization ensures that only authorized and compliant devices are allowed to connect to ground segment networks. NAC solutions authenticate devices at the point of entry, wired, wireless, or VPN, and validate attributes such as patch level, security software status, and configuration compliance before granting access.
	NET-11	**Network Operations Center**	A Network Operations Center (NOC) monitors network availability across the ground segment to ensure mission support. The capability coordinates maintenance, outage response, and telemetry for reliable operations.
	NET-12	**Network Time Protocol**	Network Time Protocol (NTP) keeps systems synchronized to authorized time sources. Accurate, authenticated time underpins logging, crypto, and coordinated operations.
	NET-13	**Port Security**	Port security restricts physical switch ports to known devices and behaviors. It blocks rogue attachments through MAC limits, authentication, and shut/quarantine actions.
	NET-14	**Segmentation**	A practice of dividing a network into multiple isolated segments or subnets to enhance security and manageability. These capabilities support traffic isolation to limit lateral movement of threats and to enforce security policy in network segments.
	NET-15	**Simple Network Management Protocol (SNMP)**	Simple Network Management Protocol (SNMP) enables device monitoring and management. Secure deployments require SNMPv3 with strong authentication and encryption.
	NET-16	**Trunking**	Trunking carries multiple VLANs over a single link to interconnect segments. Controlled tagging and policies prevent VLAN hopping and misconfiguration risk.
	NET-17	**Remote Management Access**	Remote Management Access governs how administrators connect to and control network devices such as routers, switches, and firewalls from afar. Because these interfaces provide high levels of privilege, they are a common target for adversaries.
	NET-18	**Web Proxy**	Web proxies broker outbound web access and apply security policy. They filter content, inspect TLS, log usage, and block malware and data exfiltration attempts.
	NET-19	**Wireless**	Wireless networking provides mobility for users and devices, but it also increases the network attack surface. Ground networks must have specific protection for these deployments by using controls such as strong authentication, traffic management, and continuous posture checks.
Computer Network Defense / Incident Response (CND/IR)	**CND-1**	**Digital Forensics**	Forensics is the disciplined process of collecting, preserving, and analyzing digital evidence to understand security incidents within a ground segment. Forensics involves capturing artifacts such as logs, memory, disk images, and network traffic to reconstruct attacker actions, determine root causes, and assess the scope of compromise.
	CND-2	**Hunting**	Threat hunting is a proactive search for adversaries already present but undetected. This capability combines telemetry analysis, hypotheses, and intel-driven leads to find stealthy activity.
	CND-3	**Threat Intelligence**	Threat intelligence provides curated indicators, behaviors, and context about adversaries. The intelligence informs detection engineering, hunting, and prioritized defenses.
	CND-4	**Intrusion Detection and Prevention Systems**	Intrusion detection and prevention systems (IDPS) monitor network traffic for malicious patterns and behaviors. The systems alert and block suspicious activity to contain compromises quickly.
	CND-5	**Incident Response Policy / Procedures**	Incident response establishes roles, responsibilities, communication flows, and detailed actions to manage security events. The policy and procedures coordinate detection, containment, eradication, and recovery from security incidents. This approach also emphasizes continuous improvement based on post-incident analysis.
	CND-6	**Security Sensors**	Security sensors are deployed across multiple DiD layers to capture real-time security telemetry (e.g., network traffic, endpoint activity, application logs) that aassistin threat detection, forensic investigations, and continuous security monitoring.
	CND-7	**Security Information & Event Manager**	A Security Information & Event Manager (SIEM) aggregates and analyzes logs from across the mission to detect threats and support investigations. Correlation rules and analytics turn raw events into actionable alerts.
	CND-8	**Security Operations Center**	A Security Operations Center (SOC) performs security-focused continuous monitoring and incident handling. The SOC integrates tooling, processes, and people to defend the mission in real time.

	CND-9	**Test Access Points**	Test Access Points (TAPs) are hardware or virtual mechanisms that provide a dedicated, reliable copy of network traffic for monitoring and analysis. Unlike mirror ports that may drop packets under load, TAPs deliver complete visibility into communications without disrupting live operations.
Perimeter	**PER-1**	**Web Application Firewall**	A Web Application Firewall (WAF) protects web apps from exploitation and abuse. The capability inspects requests, enforces policies, and blocks common and emerging attacks at the edge.
	PER-2	**Virtual Private Network / Remote Access**	Virtual Private Network (VPN) and Remote Access provide secure connectivity for users and administrators who need to reach mission ground systems from outside trusted facilities. VPNs create encrypted tunnels that protect the confidentiality and integrity of data in transit, while access controls such as multi-factor authentication and device posture checks ensure only authorized, compliant users, and systems connect.
	PER-3	**Data Loss Prevention – Perimeter**	DLP encompasses technologies and policies that monitor, detect, and control the movement of sensitive information leaving ground segment networks. By inspecting email, web traffic, file transfers, and cloud services, DLP helps prevent accidental leaks or deliberate exfiltration of critical data such as ITAR-controlled information, credentials, or mission telemetry.
	PER-4	**Demilitarized Zones / Security Zones**	Demilitarized Zones (DMZs) and security zones isolate externally exposed services from internal mission networks. The design reduce exposure by strictly controlling traffic between zones.
	PER-5	**Perimeter Firewall**	Perimeter Firewalls are security devices or services that control traffic entering and leaving ground segment networks. The capabilities enforce rules based on IP addresses, ports, protocols , creating a barrier between trusted internal systems and untrusted external environments.
Physical	**PHY-1**	**Badging / Doors**	Badging and door control govern who can physically enter sensitive spaces. They combine credentials, policies, and anti-tailgating measures to prevent unauthorized access.
	PHY-2	**Fire Suppression**	Fire suppression protects facilities and equipment from fire without causing undue damage. Detectors, suppression agents, and maintenance ensure availability and safety.
	PHY-3	**Gates/Guards**	Gates and guards secure site perimeters against unauthorized vehicles and persons. They verify personnel credentials, enforce procedures, and respond to incidents.
	PHY-4	**Logging - Physical**	Visitor Access Logging records the entry and exit of all personnel and visitors into secure facilities. These logs create an accountability trail that supports escort policies, enforces compliance requirements, and aids investigations when security incidents occur.
	PHY-5	**Mission Security Personnel**	Mission security personnel provide on-site protection for people, facilities, and operations. They deter threats, coordinate response, and integrate with cyber operations as needed.
	PHY-6	**Infrastructure Diversity**	Infrastructure diversity distributes critical services across independent locations and utilities. This capability limits single points of failure and supports continuity of operations.
	PHY-7	**Surveillance**	Surveillance provides visual monitoring of perimeters and sensitive areas. Recorded and live video enhances deterrence, detection, and forensic reconstruction.
Prevention	**PRE-1**	**Personnel Awareness**	Personnel awareness builds a vigilant workforce able to spot and report anomalies. Campaigns, drills, and clear reporting channels strengthen organizational security culture.
	PRE-2	**Personnel Management**	Personnel management governs the lifecycle of identities and access as people join, move, and leave. Timely provisioning and deprovisioning reduces insider risk and orphaned accounts.
	PRE-3	**Security Assessments**	Security assessments measure how well controls work and where to improve. They range from vulnerability scanning to penetration tests and red-team exercises.
	PRE-4	**Threat Assessment**	Threat assessment evaluates adversaries, motivations, and capabilities relevant to the mission. It drives prioritization of defenses and informs design and operations decisions.
	PRE-5	**End-user Training**	End-user training teaches personnel how to operate securely and resist social engineering. Role-based content and realistic exercises raise readiness for mission-specific threats.

	PRE-6	**Information Security Staff Training**	Information Security staff training develops the specialized skills defenders need to protect the mission. It includes advanced courses, certifications, and hands-on exercises tied to mission systems.
	PRE-7	**Supply Chain - Prevention**	Supply chain security protects against tampering, counterfeit components, compromised code, and overall vulnerable components from suppliers. The supply chain spans procurement, integration, maintenance, and lifecycle management of mission-critical hardware, software, and services.

Appendix B: Baseline and Enhanced Countermeasures

Table 2 provides Baseline and Enhanced countermeasure explanations for each sub-layer.

Table 2 - DiD Sub-layer Countermeasure Tiers

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
DAT-1	Strong authenticated cryptographic protections shall be applied to mission, management, telemetry, timing, and control-plane data wherever it traverses IP networks or crosses trust boundaries. AES-256 encryption shall be enforced for data at rest across storage arrays, databases, telemetry archives, logs, firmware repositories, endpoint drives, and mission systems within Ground Stations, MOC servers, and Launch integration consoles. Data in transit shall be protected using TLS 1.2 or higher with strong cipher suites for internal APIs, command sequencing paths, telemetry feeds, ephemeris and TLE distribution, tracking data, configuration distribution, remote administration channels, and partner connectivity. ICS and launch-pad OT systems that rely on legacy protocols shall be protected through VPN overlays, IPSec, MACsec, or equivalent network-layer encryption to ensure valve control, fueling systems, ACU control channels, and SCADA communications are not susceptible to interception or manipulation. Authenticated time distribution mechanisms such as NTS for NTP or authenticated PTP profiles shall be implemented to protect against time spoofing. Cryptographic key management shall be centrally controlled using HSM-backed solutions, with key rotation occurring at least quarterly or aligned to mission lifecycle requirements. All key usage shall be logged and auditable. Cryptographic material, credentials, API keys, OAuth tokens, session cookies, and signing artifacts shall be encrypted at rest and protected during transport using secure key exchange mechanisms such as Key Management Interoperability Protocol or Public Key Cryptography Standards. Encryption at the Moderate level is intended to materially reduce exposure to adversary-in-the-middle attacks, network sniffing, credential theft, data manipulation, remote service exploitation, and replay attempts by ensuring confidentiality and integrity protections are applied across the control plane, telemetry plane, and management plane of the mission architecture.	Encryption becomes a continuously enforced, hardware-rooted mission assurance control rather than a transport safeguard. All cryptographic implementations shall utilize FIPS-validated modules across mission systems, including ICS controllers, telemetry processors, ground infrastructure, and launch environments. TLS 1.3 shall be required for all applicable interfaces, with mutual authentication, certificate pinning, strict cipher enforcement, anti-downgrade protections, and short-lived session keys. Internal network segments shall not be assumed trusted; encryption and authenticated integrity protections shall be enforced across all internal pipelines and cross-domain transfers. All mission cryptographic material, including uplink keys, command authentication keys, signing certificates, and telemetry protection keys, shall be generated, stored, and managed exclusively within hardware security modules and shall never exist in plaintext outside controlled cryptographic boundaries. Cross-domain solutions shall sanitize, validate, and encrypt all data leaving mission enclaves. Secure boot, firmware signing, and authenticated update mechanisms shall be cryptographically enforced. Authenticated and integrity-protected DNS, time distribution, telemetry ingestion pipelines, sensor-to-SIEM feeds, threat intelligence exchanges, forensic artifact transfers, and partner federation links shall be continuously monitored for cryptographic health and configuration compliance. Security operations centers shall validate encryption posture in real time, alerting on cipher downgrades, certificate misuse, anomalous key access patterns, expired certificates, or unexpected encryption state deviations. Post-quantum cryptographic readiness planning and hybrid key exchange testing shall be incorporated into mission crypto strategy to ensure long-term resilience. At this level, encryption compromise, key misuse, or cryptographic integrity failures shall trigger automated containment or protective actions to preserve mission command integrity and telemetry authenticity. Encryption at the High level ensures confidentiality, integrity, authenticity, and non-repudiation across all mission data flows and is engineered to withstand sophisticated adversarial attempts to manipulate, intercept, replay, downgrade, or weaken cryptographic protections across space, ground, launch, and partner ecosystems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
DAT-2	Data Loss Prevention (DLP) controls shall be implemented across endpoints, network egress points, and distribution boundaries to prevent accidental or unauthorized exposure of sensitive mission data. Endpoint and perimeter DLP solutions shall inspect outbound email, USB transfers, file uploads, VPN sessions, SSH transfers, API calls, and collaboration platforms for mission-specific sensitive content, including cryptographic material, command dictionaries, telemetry files, orbital ephemeris, mission schedules, configuration artifacts, and ITAR-controlled data. DLP controls shall be applied at key vault export paths, HSM interfaces, cryptographic management services, archive systems, and distribution gateways to detect and block unauthorized attempts to copy, export, or transmit private keys, certificates, credentials, or mission artifacts. Watermarking and digital fingerprinting techniques shall be used to uniquely identify mission files and enable detection of unauthorized redistribution. At launch and fueling facilities, portable media shall be restricted or prohibited in operational zones, and content filtering shall be applied to outbound RF data processors and telemetry distribution systems. DLP policies shall monitor bulk reads, abnormal archive access, or suspicious export patterns from telemetry repositories and mission planning systems. Automated enforcement mechanisms shall quarantine suspect transfers and generate SOC alerts for investigation. Personnel shall receive regular training on proper handling of classified, proprietary, or controlled mission data. DLP findings and leakage risks shall be incorporated into mission readiness reviews. At this level, DLP serves as a last-line safeguard against insider misuse, credential theft, bulk telemetry exfiltration, and cryptographic key compromise once preventive controls have been bypassed.	Data Loss Prevention becomes context-aware, adaptive, and tightly integrated with insider threat monitoring, cryptographic governance, and cross-domain enforcement. DLP systems shall perform contextual inspection of mission-specific data types, including telemetry file formats, command payload structures, orbital prediction datasets, and cryptographic key artifacts, rather than relying solely on keyword matching. Behavioral analytics shall identify anomalous export activity, abnormal API-based telemetry access, unusual bulk data reads, or staged exfiltration through trusted VPN, firewall, or partner channels. All attempted exports of mission-critical data, including uplink keys, private certificates, orbital ephemeris, command libraries, and launch communication material, shall be cryptographically logged and correlated with insider-threat monitoring programs. Multi-party approval workflows shall be required for export of mission-critical datasets. Deception artifacts, honey files, or instrumented decoy records shall be deployed within file shares and archives to detect malicious insider reconnaissance or unauthorized collection behavior. All partner and enterprise connectivity shall traverse isolation gateways that sanitize, inspect, and validate outbound data before it leaves enclave boundaries. DLP enforcement shall apply to storage systems, APIs, telemetry pipelines, cloud services, and collaboration platforms to constrain large-scale exfiltration attempts via command-and-control channels, alternate protocols, or abuse of valid accounts. SOC correlation engines shall continuously evaluate exfiltration patterns and trigger automated containment actions when anomalous data movement is detected, including session termination, account suspension, or enclave isolation where appropriate. At this level, DLP is engineered to prevent escalation from localized compromise to systemic loss of communications trust, telemetry confidentiality, or launch mission integrity.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
DAT-3	Role-Based Access Control (RBAC) shall be enforced across all mission systems to ensure operators, administrators, contractors, automation services, and partner identities are granted access only to mission data aligned with defined job duties and system responsibilities. Default or shared accounts shall be replaced with named identities, and centralized identity management services such as Active Directory or LDAP shall be integrated with multi-factor authentication for all privileged and mission-impacting roles. Quarterly entitlement reviews shall be conducted to validate access appropriateness, and service accounts shall be segregated from user accounts with clearly defined least-privilege policies. RBAC enforcement shall restrict write and modification access to antenna pointing inputs, RF routing tables, polarization modes, calibration parameters, beam pattern tables, command sequences, payload parameters, schedules, orbital models, telemetry products, ephemeris files, archives, launch sequencing artifacts, and abort rule sets. Access to cryptographic key stores, IAM policy repositories, configuration management systems, patch repositories, firmware images, DNS zones, DHCP scopes, IP address management databases, and time configuration data shall be limited to explicitly authorized roles. For Launch and OT environments, operator-only roles with read/write segregation shall be required for PLCs, SCADA systems, controller configurations, sensor setpoints, and supervisory interfaces to limit the blast radius of compromised credentials. Access to telemetry views, anomaly outputs, network monitoring dashboards, SIEM indices, detection content, SOAR playbooks, IR case artifacts, and forensic repositories shall be tightly restricted to prevent unauthorized alteration or suppression of mission evidence. Logging of all access attempts to sensitive data stores shall be enabled and reviewed daily during launch campaigns and other high-risk operational periods. At this level, RBAC enforces least privilege to reduce exposure to data manipulation, abuse of valid accounts, unauthorized schedule modification, and insider misuse across space, ground, and launch ecosystems.	Access control transitions from static role assignment to dynamic, Zero Trust-aligned enforcement using Attribute-Based Access Control (ABAC) with continuous validation of user, device, and mission context. Access decisions shall incorporate contextual attributes such as device posture, physical location, launch phase, subsystem role, operational state, and risk signals to determine real-time authorization for reading or modifying mission data. Privileged roles shall be provisioned using just-in-time (JIT) access mechanisms and automatically revoked immediately after task completion. For safety-critical OT systems and launch command paths, dual-operator approval mechanisms or two-person control models shall be enforced for modification of command products, abort logic, cryptographic configurations, antenna pointing inputs, and other high-impact control data. ABAC policies shall govern who may view, modify, rotate, or export cryptographic keys, certificate stores, telemetry archives, detection logic, correlation rules, DNS/DHCP/IPAM records, firmware artifacts, and mission configuration templates. Permissions shall be dynamically tied into SIEM and SOAR pipelines for real-time anomaly detection and automated response, including immediate session termination or credential revocation upon detection of suspicious behavior. HR separation events and role changes shall trigger automated access revocation within minutes. Partner and enterprise identities shall be constrained to explicitly authorized datasets through context-aware enforcement at API, storage, and collaboration boundaries, limiting blast radius when valid accounts are abused. Deletion, suppression, or modification of monitoring data, IR artifacts, deception metadata, or detection logic shall require elevated and auditable approvals. At this level, RBAC and ABAC collectively serve as mission integrity controls that prevent unauthorized modification of authoritative data, reduce the blast radius of compromised credentials, and dynamically enforce least privilege across mission operations, launch systems, partner exchanges, and cyber defense infrastructure.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
DAT-4	Heightened access controls shall be applied to mission-critical artifacts whose integrity, confidentiality, or availability directly determines communications trust, launch safety, or mission continuity. Multi-factor authentication shall be required for access to sensitive repositories including command dictionaries, maneuver scripts, orbital correction plans, cryptographic key stores, certificate repositories, firmware images, boot artifacts, telemetry archives, and authoritative mission configuration datasets. Two-person approval workflows shall be enforced for retrieval or modification of highly sensitive artifacts such as mission keys, abort rule sets, launch command sequences, hopping/nulling configurations, PLC logic, interlock parameters, and other safety-critical operational data. Sensitive folders, repositories, and storage volumes shall enforce “default deny” ACLs with explicit authorization requirements. Engineering consoles and Launch OT systems shall restrict access to authorized roles only, with enhanced logging, session recording, and traceability during countdown and fueling operations. Access to authoritative telemetry datasets, anomaly outputs, validated time references, integration test results, and acceptance artifacts shall require elevated auditing to prevent silent manipulation. Cryptographic material, trust anchors, token signing keys, and HSM configuration objects shall be protected with enhanced access logging and approval gates to reduce risk of key theft or misuse. Access reviews shall be conducted prior to major mission milestones such as launch readiness reviews or countdown initiation. Personnel handling sensitive mission artifacts shall receive focused training and escalation playbooks to ensure proper custody, approval routing, and anomaly reporting. At this level, Sensitive Data Access Control reduces insider threat risk and limits the impact of compromised credentials by ensuring that mission-critical artifacts cannot be altered, exported, or corrupted without additional authentication, approvals, and auditing.	Sensitive data access enforcement becomes context-aware, cryptographically bound, and tamper-evident. Attribute-Based Access Control (ABAC) policies shall dynamically govern access to mission-critical artifacts based on mission phase, time of day, launch state, device posture, enclave location, and operational risk signals. Access to cryptographic material, launch command logic, maneuver planning inputs, safety interlock configurations, authoritative telemetry truth datasets, and defensive configurations shall require hardware-backed certificate authentication using trusted hardware tokens or secure enclave-backed credentials. All sensitive data access or export requests shall trigger workflow approvals requiring cryptographic signatures from authorized approvers, with SOC visibility and correlation into insider threat monitoring systems. Dual-control enforcement shall apply to high-impact modifications such as abort logic changes, trust anchor updates, RF control parameter adjustments, firmware image promotion, or modification of detection logic and response playbooks. Immutable, tamper-evident logging mechanisms shall be used for sensitive data access events, with cryptographically verifiable audit trails to prevent alteration or deletion of evidence. Secure enclave execution shall be required for cryptographic operations involving private keys, certificate signing material, token introspection secrets, and trust anchors. Memory-hard key derivation functions and hardened credential storage mechanisms shall be enforced for all sensitive authentication material. Cross-enclave data exchanges, including Ground Station to Mission Operations Center transfers or partner mission artifact sharing, shall traverse controlled cross-domain solutions with enforced sanitization, inspection, and encryption. Access to authoritative telemetry truth, security alerts, vulnerability findings, forensic artifacts, and threat intelligence repositories shall require elevated controls to prevent stealthy manipulation of situational awareness. At this level, Sensitive Data Access Control functions as a mission integrity preservation mechanism, ensuring that compromise of a user account, partner connection, or subsystem does not translate into silent corruption of authoritative mission data, safety-critical configurations, or cryptographic trust foundations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-1	Configuration control shall enforce centralized, controlled, and repeatable build processes for all mission software, firmware, dashboards, telemetry processors, anomaly detection engines, planning tools, command sequencing applications, and infrastructure-as-code artifacts. All source code shall reside in centrally managed version control systems with signed commits and controlled access. Build pipelines shall execute in automated, reproducible environments using containerized or virtualized infrastructure to reduce configuration drift and prevent unauthorized toolchain substitution. All build artifacts (e.g., including binaries, scripts, firmware images, containers, configuration packages, and model parameters) shall undergo integrity verification through cryptographic hash or signature validation prior to deployment. Deployed artifacts shall be traceable to approved source repositories and authorized toolchains to ensure provenance. Launch OT and ICS firmware, including PLC logic, SCADA components, ACU control software, transceiver firmware, and relay routing logic, shall require vendor-provided signed binaries validated at deployment. Custom signal-path controllers, calibration software, and defense algorithms shall only be promoted after integrity validation. Configuration baselines for Mission Operations Center servers, Ground Station telemetry processors, dashboard systems, and update tooling shall be automated and monitored for deviation. Unauthorized changes to command parsers, dictionary files, abort logic, relay firmware, test harnesses, validation scripts, and embedded GSE logic shall be detected and remediated prior to operational use. At this level, configuration control reduces exposure to supply-chain compromise, malicious script insertion, unauthorized algorithm modification, firmware tampering, and trust-control bypass before software reaches operational mission environments.	Configuration control enforces cryptographically verifiable software provenance and tamper-resistant promotion workflows across all mission build pipelines. All build outputs shall be cryptographically signed with verifiable attestations recorded in immutable logging systems, ensuring that deployed artifacts can be traced to specific source commits, build environments, and authorized toolchains. Reproducible build techniques shall be validated through independent verification processes to ensure identical outputs from identical source states. Promotion of software, firmware, configuration templates, containers, planning tools, launch sequencing code, abort logic, relay firmware, PLC logic, SCADA components, and cryptographic services into operational environments shall require dual authorization. Secure boot mechanisms with firmware signing shall be enforced for OT and ICS controllers at launch pads and mission-critical ground facilities, preventing execution of unauthorized firmware images. Supply-chain integrity frameworks such as Supply-chain Levels for Software Artifacts (SLSA) or equivalent provenance models shall be integrated into the build lifecycle to protect against dependency poisoning, upstream package compromise, and malicious injection into CI/CD pipelines. Build environments, signing services, and artifact repositories shall themselves be hardened and monitored as high-value assets. Red-team assessments and adversary emulation shall be conducted against the build pipeline to test for malicious injection scenarios, including insider manipulation of source repositories, tampering with build scripts, substitution of toolchains, corruption of signing keys, or unauthorized modification of firmware prior to deployment. At this level, configuration control establishes a cryptographic root-of-trust for mission software and firmware, ensuring that operational binaries, control logic, and cryptographic services are derived solely from authorized source code and approved build environments, and preventing adversaries from inserting persistent, pre-deployment logic into mission systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-2	Language-specific secure coding standards shall be formally defined and enforced for all mission software components, including TT&C applications, telemetry parsers, dashboards, launch sequencing software, planning tools, automation scripts, anomaly detection plugins, and CI/CD tooling. Standards shall be mapped to relevant Common Weakness Enumerations (CWEs) applicable to mission environments (e.g., input validation, memory safety, bounds checking, authentication and authorization logic, cryptographic use, error handling, logging integrity) and secure dependency management. Strict input validation and robust parsing requirements shall apply to telemetry decoding, command entry GUIs, update orchestration mechanisms, and exposed APIs to prevent malformed-input exploitation, injection, script abuse, and trust-boundary violations. Command and scripting interfaces shall enforce syntactic and semantic validation to prevent execution of unsafe but syntactically valid inputs. Secure error handling shall ensure that ICS and OT controllers at launch pads fail safely and predictably without exposing debug data, bypassing authorization, or entering unsafe operational states. Standards shall require authenticated update verification, explicit trust-boundary validation, and controlled deserialization to prevent malicious plugin insertion or compromised update artifacts. Peer review processes shall include security checklists, and at least one automated static analysis or linter tool shall be integrated into the CI/CD pipeline to detect violations prior to merge or release. Secure coding standards shall be reviewed and updated at least annually based on lessons learned from assessments, red-team exercises, and threat intelligence. Developers shall receive training aligned with relevant adversary TTPs (ATT&CK, SPARTA) to ensure awareness of how coding flaws translate into exploitable mission risks. At this level, secure coding standards reduce the likelihood of injection vulnerabilities, malformed command execution, parser corruption, logic bypass, and unsafe failure conditions that could enable data manipulation, denial-of-service, or trust subversion in mission systems.	Secure coding compliance becomes a mandatory and enforceable gate within the development lifecycle. All commits shall be subject to automated compliance checks, and builds shall fail if coding standards are violated. Multiple advanced static analysis tools shall be integrated into CI/CD pipelines and aligned to prioritized CWE lists relevant to mission-critical software (e.g., memory corruption, injection, improper authentication logic, and insecure cryptographic usage). Where feasible, new mission-critical components shall prioritize memory-safe languages such as Rust to reduce classes of memory corruption vulnerabilities inherent in unsafe languages. Runtime sanitizers and fuzz testing shall be required for telemetry decoders, command parsers, scheduling APIs, launch software, and automation interfaces to detect edge-case parsing failures, bounds errors, and unsafe execution paths that static analysis alone cannot identify. Secure coding standards shall mandate strict control of embedded scripting engines, automation hooks, and plugin architectures to prevent abuse of command interpreters and unsafe extension mechanisms. Web dashboards and visualization engines shall enforce secure rendering logic, input sanitization, state validation, and protection against defacement or content manipulation attacks. Developers shall be required to complete formal secure coding training or certification prior to receiving commit privileges for mission-critical repositories. Secure coding compliance metrics shall be tracked and reported as part of mission readiness assessments. At this level, secure coding standards operate as a proactive mission assurance control, systematically eliminating exploitable injection flaws, memory safety violations, logic bypass conditions, unsafe update paths, and trust-boundary weaknesses before software reaches build pipelines or operational deployment.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-3	Mission software development shall prioritize prevention of high-risk Common Weakness Enumeration (CWE) classes that are directly aligned with mission threats and operational impact. Weakness classes such as buffer overflows and memory safety violations, improper authentication and authorization, improper input validation, unsafe deserialization, race conditions, and logic bypass conditions shall be formally identified as high-priority for mission systems. Automated scanning profiles within CI/CD pipelines shall explicitly target prioritized CWE classes relevant to TT&C software, telemetry decoders, command parsers, dashboards, planning tools, launch sequencing applications, and exposed APIs. Secure coding enforcement shall include test cases designed to validate mitigation of each prioritized CWE before deployment. Special emphasis shall be placed on preventing parser corruption, malformed-input exploitation, unchecked scripting, improper validation of telemetry ingestion pipelines, and unsafe file-handling behaviors that could enable remote exploitation or denial-of-service. For ICS and OT firmware, vendor validation shall be required to demonstrate mitigation of high-risk weakness classes prior to integration into launch or operational environments. SOC monitoring shall integrate awareness of vulnerable service behaviors, including logging anomalies associated with services historically affected by prioritized CWE classes. At this level, CWE prevention reduces exploitability of exposed mission software and control-plane services by systematically blocking common, high-impact weakness classes before operational deployment.	CWE prevention is formalized through structured threat modeling and runtime enforcement aligned to mission-specific adversary techniques. Formal threat models shall map prioritized CWE classes to relevant ATT&CK and/or SPARTA techniques and mission attack scenarios, ensuring that mitigation efforts directly address realistic exploitation paths. Runtime defensive mechanisms such as stack canaries, address space layout randomization (ASLR), control-flow integrity, memory protection mechanisms, and hardened compilation flags shall be required for mission-critical components and validated through testing. Advanced static analysis and taint-tracking techniques shall be applied across codebases to detect unsafe propagation of telemetry inputs, command parameters, and user-controlled data across trust boundaries. Vendors supplying OT firmware, control software, dashboards, or telemetry processors shall provide documented evidence of mitigation for prioritized CWE classes prior to acceptance. Adversary emulation campaigns and red-team assessments shall be conducted to validate that mitigations for injection, parser corruption, authentication bypass, unsafe state handling, and deserialization weaknesses withstand realistic exploitation attempts. Continuous security dashboards shall track prioritized CWE classes, open findings, remediation status, and residual mission risk, providing leadership visibility into weakness trends across mission components. At this level, CWE prevention operates as a measurable, threat-informed assurance mechanism that actively reduces systemic software exploitability across mission command, telemetry processing, launch systems, and OT environments.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-4	An authoritative inventory shall be maintained for all software platforms, applications, services, firmware, container images, virtual machines, and mission-specific code deployed across Ground Station, Mission Operations, Launch, Networking, Security Operations, and supporting infrastructure. Authoritative system-level documentation shall be maintained to describe software modules, data flows, control paths, trust boundaries, and interface dependencies across mission systems. Architecture diagrams shall illustrate telemetry ingestion pipelines, parser logic, databases, operator consoles, command validation gates, sequencing tools, abort logic paths, update workflows, and rollback mechanisms. Documentation shall provide a shared source of truth for engineering, assessment, and incident response teams. Diagrams shall be updated prior to each major mission phase, including launch campaigns and significant software changes, and stored in a version-controlled repository accessible to authorized mission personnel. Role-based access controls shall restrict sensitive architectural details such as cryptographic key flows, command handler internals, authentication mechanisms, and OT control interfaces to appropriate roles. Staff shall be trained on how to use architectural documentation during anomaly response, particularly under time-compressed launch conditions where clear understanding of control flow and data dependencies is essential. At this level, software documentation reduces the likelihood of misconfiguration, trust subversion, and delayed incident response by ensuring that authoritative system architecture and data-flow knowledge is readily available and accurate.	For the collected software inventory, it shall record software name, version, vendor, cryptographic hash, host system, mission function, approval status, installation date, patch level, dependencies, and assigned owner. Automated asset discovery tools shall continuously enumerate installed and executing software and reconcile findings with the approved inventory. Unauthorized, unapproved, outdated, or rogue software shall trigger investigation, containment, and removal procedures. Software inventory shall be integrated into configuration management, vulnerability management, and mission readiness processes. Architecture documentation becomes cryptographically controlled, continuously validated, and directly integrated into mission assurance and threat modeling workflows. All architectural diagrams, data-flow models, and control-flow descriptions shall be version-controlled, cryptographically signed, and validated against live system configurations to ensure alignment between documented and deployed states. Automated discovery mechanisms shall be used to map actual data flows, service dependencies, API connections, and OT interfaces, with discrepancies flagged for review. Immutable architecture baselines shall be preserved for forensic use, enabling investigators to compare operational states against known-good configurations following integrity or trust-subversion incidents. Red-team validation shall be conducted to ensure documentation accurately reflects exploitable paths, including undocumented interfaces, backdoor communications channels, shadow services, or untracked OT integrations. Architecture artifacts shall be formally integrated into launch readiness reviews and anomaly response playbooks. Dynamic threat modeling tools shall be linked to architecture documentation, enabling mapping between software components, trust boundaries, adversary techniques, and defensive controls. At this level, documentation is not merely descriptive as it is an actively validated mission integrity asset that supports rapid recovery, trust restoration, and defensible decision-making during high-impact operational events.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-5	Dynamic analysis testing shall be conducted in flight-like or operationally representative environments to identify runtime failures, logic flaws, unsafe state transitions, malformed data handling issues, and resource-exhaustion conditions that are not detectable through static analysis alone. Command parsers, telemetry decoders, scheduling APIs, gateway services, visualization platforms, and TT&C software shall undergo fuzz testing and malformed input testing to evaluate resilience against unexpected or adversarial inputs. Digital twin or simulation environments shall be used to exercise spacecraft and OT systems under injected faults, replayed commands, corrupted telemetry frames, timing edge cases, and abnormal approval sequences to observe crash conditions, unsafe behaviors, or denial-of-service states. Launch software, telemetry visualization systems, and mission control interfaces shall be stress-tested under peak operational load to ensure resilience against runtime manipulation and endpoint service degradation. OT components including PLCs, SCADA firmware, HMIs, and supervisory control services shall be incorporated into lab-based dynamic testing harnesses to evaluate behavior under malformed inputs and abnormal load conditions. Regression testing shall be applied to patched systems and updated firmware to ensure fixes do not introduce new runtime vulnerabilities. All anomalies, unsafe states, and failure conditions identified during dynamic testing shall be documented along with mitigation actions and tracked to closure. At this level, dynamic analysis testing is intended to reduce exposure to runtime manipulation, script abuse, approval bypass attempts, malformed command injection, endpoint denial-of-service, and service interruption conditions that could impact mission availability or operational safety.	Dynamic analysis testing becomes adversarial driven and integrated into mission readiness, launch certification, and continuous integration pipelines. High-fidelity digital twins of spacecraft, launch systems, and OT environments shall provide full visibility into memory, process state, control logic transitions, timing behavior, and interface boundaries to enable deep runtime inspection under abuse conditions. Adversarial fault-injection campaigns and coordinated red-team exercises shall be conducted against TT&C software, telemetry ingestion pipelines, launch control systems, scheduling APIs, gateways, and supervisory OT interfaces to intentionally induce malformed commands, timing manipulation, approval bypass attempts, memory corruption conditions, and resource exhaustion scenarios. Continuous fuzzing of mission-critical parsers, protocol handlers, and control-plane services shall be embedded into CI/CD pipelines to detect runtime instability before deployment. Dynamic testing shall include validation of memory handling, boundary enforcement, process isolation, and error-handling logic to identify exploitable crash states, unsafe failover behavior, or logic flaws that could enable runtime manipulation or denial-of-service during peak operations. Vendors supplying OT devices, firmware, or supervisory control systems shall be required to participate in fuzz testing, memory exploitation validation, and runtime resilience validation prior to launch readiness approval. All findings from adversarial dynamic testing shall be formally incorporated into mission risk registers, launch readiness reviews, and system hardening plans. At this level, dynamic analysis testing is treated as a mission assurance control that proactively identifies exploitable runtime weaknesses before adversaries can weaponize them against command paths, telemetry processing pipelines, or safety-critical launch systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-6	Software supply chain risk management shall require generation and maintenance of Software Bills of Materials (SBOMs) for all mission software components, including ground applications, telemetry processors, dashboards, CI/CD artifacts, and OT firmware packages deployed to launch pads, Mission Operations Centers, or Ground Stations. SBOMs shall document third-party libraries, dependencies, firmware components, scripting engines, containers, and update mechanisms to ensure visibility into upstream components. Leverage SBOM provenance information through enrichment activities that assess supply chain risk (e.g., CVEs, foreign influence, secure software development). Dependency sources shall be validated against trusted repositories, and all packages, containers, and firmware images shall undergo vulnerability scanning for known Common Vulnerabilities and Exposures (CVEs) prior to deployment. Vendor-provided firmware updates, including ACU software, SDR firmware, switching controllers, amplifier control software, relay drivers, and launch sequencing modules, shall require vendor signing and integrity verification before installation. Periodic dependency reviews shall be conducted prior to major mission phases, including launch campaigns, to assess exposure to known vulnerabilities or supply chain risk indicators. Third-party orbital models, telemetry libraries, decompression tools, and science processing toolchains shall be reviewed for provenance and trustworthiness to prevent introduction of malicious logic or poisoned data inputs. The Security Operations Center shall be alerted when vulnerable dependencies remain unpatched or when high-risk components are detected in operational environments. At this level, supply chain risk management reduces exposure to upstream compromise, vulnerable libraries, malicious update artifacts, and pre-deployment insertion of compromised firmware or software components.	Supply chain risk management becomes continuous, cryptographically enforced, and deeply integrated into deployment gating and vendor governance processes. SBOMs shall be continuously validated against live system deployments to ensure that operational environments precisely match documented dependency inventories. Cryptographic provenance verification and signed attestations shall be required for all software artifacts, containers, firmware images, and dependency chains within CI/CD pipelines. Deployment shall be automatically blocked if any dependency lacks verified provenance, valid cryptographic signatures, or approved pedigree documentation. Third-party audits of dependency chains shall be required for mission-critical systems, including launch sequencing libraries, OT firmware, telemetry ingestion frameworks, cryptographic libraries, and detection tooling. Vendor-supplied firmware, PXE boot artifacts, provisioning tools, and management utilities shall require SBOM submission and signed attestation prior to integration into launch pad systems or Mission Operations infrastructure. Cryptographic libraries and key management dependencies shall undergo enhanced scrutiny to prevent weakened or malicious components from undermining encryption enforcement. Supply chain controls shall extend to CI/CD plugins, model training datasets, emulation frameworks, detection content packs, and red-team tooling to prevent poisoned toolchains or compromised automation components from becoming intrusion vectors. Continuous dashboards shall correlate SBOM data with CVE feeds, foreign influence indicators, vulnerability intelligence, and mission risk scoring. At this level, software supply chain risk management functions as a proactive integrity control that prevents introduction of malicious firmware, backdoored libraries, poisoned dependencies, weakened cryptographic components, and compromised toolchains before they reach operational mission systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-7	Static application security testing (SAST) shall be integrated into CI/CD pipelines for all custom-developed or mission-tailored software across the ground segment. This includes Mission Operations Center command and control applications, mission planning and scheduling tools, telemetry ingestion and decoding services, engineering dashboards, anomaly detection plugins, launch sequencing applications, launch monitoring visualization systems, Ground Station antenna control logic, signal-conditioning supervisory software, automation scripts, infrastructure-as-code templates, GaaS command and telemetry gateways, and network management utilities. Static analysis tools shall inspect both source code and compiled artifacts without execution to identify unsafe coding patterns, injection risks, memory safety violations, improper authentication and authorization logic, insecure cryptographic usage, deserialization flaws, parser weaknesses, and other Common Weakness Enumeration (CWE) classes aligned to mission-prioritized risks. Rule sets shall be mapped to threat-informed CWE categories relevant to command integrity, telemetry processing, launch safety, OT control software, and externally exposed APIs. Particular attention shall be given to software components that process spacecraft commands, decode telemetry, enforce abort logic, manage PLC/SCADA interfaces, control antenna positioning, or expose customer-facing GaaS interfaces. High-severity findings shall require remediation prior to deployment into operational Mission Operations Center systems, launch integration environments, ground station production systems, or external service gateways. Scan results shall be retained and shared with mission governance and Security Operations Center functions for risk tracking and correlation with operational telemetry and threat intelligence. At the Moderate level, static analysis testing reduces the likelihood that exploitable coding flaws, unsafe parsing behavior, trust-boundary violations, or injection paths are introduced into operational mission software.	Static analysis testing becomes multi-layered, adversary-informed, and promotion-gating across all mission ground functions. Multiple advanced static analyzers shall be required for mission-critical codebases supporting Command and Control, Launch Integration and Operations, Ground Station control systems, Network Services, GaaS infrastructure, and SOC tooling. These analyzers shall incorporate deep data-flow analysis, taint tracking across trust boundaries, symbolic execution, control-flow integrity validation, and advanced detection techniques capable of identifying emerging vulnerability classes beyond traditional pattern matching. A zero-tolerance promotion policy shall be enforced for software supporting launch control systems, launch monitoring platforms, facility management PLC/SCADA interfaces, Mission Operations command stacks, cryptographic services, and GaaS command gateways. Software shall not be promoted into operational or launch pad environments if unresolved critical or high-risk findings remain. Vendor-supplied firmware and software components, including OT engineering tools, antenna control firmware, signal-conditioning controllers, and GaaS infrastructure elements, shall require documented static analysis evidence demonstrating mitigation of prioritized CWE classes prior to acceptance. Static analysis findings shall be correlated with adversary tradecraft and threat intelligence to identify vulnerable code paths consistent with known exploitation techniques. Results shall feed centralized mission risk dashboards and launch readiness reviews, ensuring software risk posture is formally assessed before operational milestones. In addition to automated scanning, adversarial code review campaigns shall be conducted against high-impact components such as command parsers, telemetry decoders, abort logic, authentication modules, cryptographic key handling services, update mechanisms, and multi-tenant gateway isolation logic. At the High level, static analysis testing functions as a preventive mission assurance control that systematically blocks exploitable weaknesses across Mission Operations, Ground Station, Launch Systems, Networking, GaaS, and SOC environments before software reaches operational deployment, aligning inspection rigor with real-world adversary exploitation patterns.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CSW-8	Structured threat modeling shall be conducted across all ground segment mission software and operational functions to identify likely adversaries, attack paths, trust boundary violations, and mission-impacting consequences. Recognized methodologies such as STRIDE and threat-informed frameworks aligned to ATT&CK and SPARTA shall be applied to Mission Operations Center command sequencing, real-time commanding systems, telemetry ingestion and decoding pipelines, scheduling and orbital prediction tools, engineering dashboards, CI/CD and infrastructure-as-code processes, Ground Station control software (antenna pointing, signal conditioning, and RF path configuration), Launch Control Center sequencing and abort logic, Launch Monitoring visualization platforms, Facility Management PLC/SCADA environments, and Ground Station as a Service (GaaS) APIs and command gateways. Threat models shall explicitly document command lifecycles, telemetry data flows, dictionary validation paths, scheduling and ephemeris handling logic, authentication boundaries, privilege transitions, update mechanisms, firmware deployment paths, and safety interlocks. The modeling process shall connect cyber attack paths directly to mission outcomes, including missed communication passes, corrupted maneuver planning inputs, falsified telemetry displays, collision risk, unintended delta-V execution, launch abort triggers, relay misconfiguration, or unsafe facility state transitions. Particular emphasis shall be placed on modeling data manipulation (T1565), masquerading (T1036), adversary-in-the-middle scenarios (T1557), trust subversion (T1553), supply chain compromise (T1195), and denial-of-service conditions affecting operational availability (T1489, T1499). Threat modeling shall cover the full data lifecycle (i.e., ingest, decode, transform, validate, archive, and distribute) to identify where falsified-but-plausible outputs could be injected or where trust checks may be bypassed. Infrastructure-as-code templates, automation scripts, and CI/CD tooling shall be explicitly treated as valid attack surfaces. Threat models shall be updated prior to major milestones, including significant software releases, launch campaigns, architecture modifications, new partner integrations, or changes to mission-critical OT systems. Artifacts shall be stored in secure, version-controlled repositories accessible to mission engineering and cybersecurity teams. Engineers shall be trained to interpret models for mitigation planning, control selection, and test-case development. At this level, threat modeling ensures that controls are selected based on realistic mission attack paths rather than abstract vulnerability categories.	Threat modeling becomes continuous, tool-assisted, adversary-validated, and operationally enforced across all ground mission functions. Threat modeling activities shall be embedded within DevSecOps pipelines such that architecture changes, firmware updates, dependency additions, API modifications, infrastructure-as-code changes, network topology shifts, or launch configuration updates automatically trigger model review and validation. Tool-assisted platforms shall correlate architecture diagrams, data-flow mappings, privilege boundaries, OT control paths, and cross-enclave interfaces with adversary techniques to identify emergent attack chains. Threat models shall explicitly analyze adversarial manipulation of command sequencing, abort logic, relay configurations, antenna pointing inputs, RF path control parameters, telemetry dashboards, mission planning outputs, cryptographic material handling, facility management safety systems, and GaaS multi-tenant command boundaries. Special emphasis shall be placed on modeling deception scenarios in which operators “believe the picture,” including falsified telemetry, suppressed alerts, manipulated engineering data, timing attacks during exercise or maintenance windows, and compromise of monitoring platforms themselves. Safety-critical OT systems shall include modeling of safety bypass (T0809), denial of control (T0855), manipulation of view (T0868), and loss-of-safety scenarios with both cyber and physical consequences. Adversary emulation and red-team exercises shall be used to validate that documented threat models accurately reflect exploitable paths in practice, including undocumented interfaces, shadow services, privilege escalation routes, cross-domain pivoting, and monitoring system compromise. External review of threat models shall be required prior to launch readiness, major operational deployment, or high-impact architecture transitions. Threat modeling outputs shall be correlated with live SOC telemetry, detection gaps, incident data, and purple-team results to validate coverage of observed tactics, techniques, and procedures. Any divergence between modeled threats and observed adversary behavior shall trigger mitigation updates and control reassessment. Threat modeling artifacts shall feed directly into mission risk registers, with formal quarterly updates reflecting architectural changes, threat intelligence evolution, supply-chain insights, and validation results. At this level, threat modeling operates as a living mission assurance mechanism that continuously aligns system design, control implementation, testing strategy, detection engineering, and operational monitoring against evolving adversary capabilities and mission-specific attack paths across Mission Operations, Ground Station, Launch Systems, Networking, GaaS, and Security Operations functions.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-1	Application whitelisting shall be enforced across all supported mission IT and hybrid IT/OT endpoints, including Mission Operations Center command and control servers, telemetry processors, mission planning systems, engineering workstations, Ground Station antenna control systems, signal conditioning management interfaces, network management consoles, launch sequencing servers, launch monitoring dashboards, security service hosts, and Ground Station as a Service (GaaS) command and telemetry gateways. Whitelisting policies shall use hash-based or publisher-based rules to allow execution only of explicitly approved mission software, including command sequencers, telemetry decoding tools, orbital planning applications, dashboard services, PLC control clients, cryptographic utilities, and authorized administrative tools. Processing hosts that perform telemetry ingestion, decoding, data transformation, archival processing, and science product generation shall be restricted to approved binaries and scheduled batch jobs to prevent unauthorized script execution or pipeline abuse associated with command interpreter misuse (T1059) and obfuscated tooling (T1027). Engineering consoles and analytics servers shall likewise be limited to approved visualization, anomaly detection, and resource modeling components to reduce exposure to unauthorized scripting or obfuscated execution paths. Launch Control Center systems, launch monitoring platforms, and sequencing stacks shall operate under a default-deny execution posture, permitting only validated launch control software, abort logic services, and approved operator interfaces. Security service hosts, including SOC collectors, SIEM components, deception systems, and DCO tooling, shall also operate under strict allowlisting to prevent compromise of defensive infrastructure. For OT environments including Facility Management PLCs, SCADA systems, antenna servo controllers, relay firmware interfaces, and fueling control systems, application allowlisting shall be applied wherever technically feasible due to the built-for-purpose nature of these endpoints. Where native agents are not supported, execution control shall be enforced at engineering workstations, HMIs, or jump hosts that mediate access to OT devices. All blocked execution attempts shall be logged and reviewed by cybersecurity personnel. Whitelisting baselines shall be periodically reviewed and updated to accommodate approved patches and version updates while maintaining strict control. At this level, application whitelisting reduces exposure to unauthorized code execution, opportunistic malware, malicious scripting, and abuse of non-approved tools across ground station, mission operations, launch infrastructure, security stacks, and GaaS environments.	Application whitelisting shall be cryptographically enforced, hardware-anchored, and continuously validated across all mission-impacting ground functions. All executables, scripts, firmware components, configuration loaders, container images, and mission-critical binaries shall require verified cryptographic code signing prior to execution. Kernel-level enforcement shall be used where supported, and secure boot processes backed by hardware roots of trust, such as TPM-based attestation or equivalent mechanisms, shall ensure that only authorized and signed software can execute at system startup and during runtime. Execution integrity controls shall apply to Mission Operations command stacks, telemetry pipelines, orbital planning engines, engineering analytics platforms, Ground Station antenna and RF management systems, Launch Control sequencing logic, launch monitoring visualization systems, Facility Management OT engineering consoles, network security appliances, SOC infrastructure, deception environments, and GaaS command gateways. Execution inventories shall be continuously validated against approved baselines to detect renamed binaries, injected libraries, interpreter abuse, or living-off-the-land evasion attempts (T1059, T1027, T1564). Whitelist modifications, including the addition of new binaries or updates to approved components, shall require dual authorization during mission-critical phases such as launch campaigns, maneuver execution windows, or high-risk operational periods. All blocked execution attempts shall generate real-time alerts into SOC and DCO pipelines for automated correlation with authentication, network, and telemetry data. Application control shall be extended to containerized workloads, orchestration agents, CI/CD runners, and infrastructure-as-code deployment tooling to prevent unauthorized build artifacts or injected automation scripts from executing in operational environments. Adversary emulation exercises shall validate that unauthorized payloads, malicious update mechanisms, injected firmware, or compromised administrative utilities cannot execute within mission-critical systems, including launch infrastructure and OT stacks. At this level, application whitelisting operates as a hardware-enforced execution integrity control that protects command and telemetry systems, prevents compromise of safety-critical OT environments, safeguards defensive security infrastructure, and limits blast radius even in scenarios involving credential compromise or partial system access during high-impact mission operations.

END-2	Comprehensive operating system and application auditing shall be enabled across all mission-supporting endpoints and control systems, including Mission Operations Center command and control servers, telemetry processors, mission planning systems, engineering workstations, Ground Station antenna control platforms, RF signal conditioning controllers, launch sequencing systems, launch monitoring dashboards, facility management PLC/SCADA engineering stations, network management hosts, GaaS gateways, and security operations infrastructure. Logs shall be forwarded to centralized Security Information and Event Management (SIEM) platforms for aggregation and correlation. Audit records shall capture user authentication events, command executions, privilege changes, configuration modifications, firmware loads, file access to mission artifacts, cryptographic operations, scheduling API calls, process execution activity, and changes to safety logic or sequencing parameters. For Ground Station systems, changes to antenna pointing state, polarization configuration, calibration parameters, RF routing tables, gain settings, nulling profiles, hop rates, DSP firmware loads, and other signal-path configuration changes shall be logged to support detection and investigation of manipulation or service disruption events. For Launch Control Center systems, logging shall capture command issuance, abort logic modifications, sequencing changes, and operator overrides. For ICS and OT environments, including fueling systems, power infrastructure, HVAC, water systems, and other facility management controls, operator actions on HMIs, PLC engineering workstations, supervisory control applications, and safety interlocks shall be logged to establish accountability and enable post-incident reconstruction of unsafe state transitions or parameter changes. Audit logs shall preserve sufficient context to reconstruct intent and system state, including timestamps, account identity, source system, and affected control element. Logs shall be protected against local tampering and forwarded to centralized storage to reduce the likelihood of suppression or deletion. Logging must also persist locally in limited form to preserve evidence in the event centralized logging infrastructure is disrupted. Logging coverage shall include network-facing services such as DNS, DHCP, IP address management, management networks, and storage services to support detection of credential misuse, lateral movement, lease abuse, record tampering, and indicator removal attempts. Logging shall also include changes to monitoring rules, playbooks, threat intelligence feeds, case records, deception configurations, and analyst actions within SOC, DCO, IR, and deception platforms to ensure the defensive stack itself remains auditable. Audit data shall be reviewed periodically, with heightened review cycles before and after launch campaigns or other mission-critical operations. Correlation between cyber events and physical state changes shall be performed where applicable, such as an authenticated session followed by antenna movement, RF configuration change, fueling valve transition, time synchronization adjustment, or abort trigger. At this level, logging and auditing provide foundational visibility, accountability, and	Logging and auditing shall operate as a real-time, tamper-resistant, cross-domain integrity assurance system spanning all mission ground functions. Endpoint and control-system audit logs shall stream continuously to centralized SIEM and analytics platforms using cryptographically validated transport and integrity controls to prevent alteration, suppression, or retroactive modification. Write-once, read-many (WORM) or equivalent immutable retention mechanisms shall be enforced for mission-critical audit records, including command execution logs, abort logic changes, cryptographic key access events, firmware promotion actions, OT control modifications, and monitoring rule updates. User and Entity Behavior Analytics (UEBA) shall be deployed across Mission Operations, Ground Station systems, Launch infrastructure, Facility Management OT, networking services, GaaS interfaces, and security tooling to establish behavioral baselines for operators, administrators, service accounts, automation processes, and API clients. Deviations from established patterns (e.g., off-cycle command issuance, anomalous antenna configuration changes, unexpected RF path manipulation, unusual scheduling overrides, abnormal PLC state transitions, unauthorized firmware uploads, or suspicious time synchronization events) shall trigger automated alerts and risk scoring. Audit data shall be enriched and correlated across IT and OT domains to detect multi-stage attack sequences, including credential misuse followed by configuration manipulation, launch sequencing modification, relay firmware updates, DNS record tampering, management network access, telemetry pipeline interference, or suppression of monitoring alerts. Cross-domain correlation shall explicitly tie cyber activity to physical state changes and operational outcomes to detect deception scenarios in which operators may be presented with falsified telemetry or manipulated views. Logging pipelines shall monitor and alert on attempts to impair defenses, including modification of SIEM rules, disabling of forwarders, alteration of DCO playbooks, tampering with deception artifacts, case record manipulation, or attempted deletion of audit logs. Time synchronization events, clock adjustments, and sync failures shall be logged and analyzed to detect time-based evasion or concealment of attacker activity. During mission-critical phases such as launch windows, maneuver execution periods, or high-risk operational transitions, high-impact security alerts affecting command systems, safety controls, cryptographic services, authoritative telemetry sources, or monitoring infrastructure shall require dual-operator review before resolution. Logging correlation shall extend across mission phases to detect pre-positioning, dormant persistence, reconnaissance, and low-and-slow manipulation attempts occurring prior to operational events. Adversary emulation and red-team validation shall confirm that stealth techniques (e.g., living-off-the-land binaries, credential abuse, unauthorized command issuance, telemetry manipulation, safety logic alteration, monitoring suppression, and attempted log tampering) produce detectable audit artifacts and cannot bypass logging pipelines. At this level, logging and auditing function as a unified cross-domain mission integrity control, ensuring that all mission-impacting actions across Ground Station, Mission Operations, Launch Systems, Networking Services, GaaS infrastructure, and Security Operations are attributable, tamper-evident,

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
	investigative capability across Ground Station, Mission Operations, Launch, Networking, GaaS, and Security Operations functions, enabling detection of manipulation, suppression, credential misuse, and insider activity affecting mission systems.	behaviorally analyzed, and operationally correlated to enable rapid detection, containment, forensic reconstruction, and trust restoration during high-impact mission events.
END-3	Strong authentication controls shall be enforced for all IT operator, administrative, engineering, and mission-impacting accounts accessing ground segment endpoints, including Mission Operations Center command and control consoles, telemetry processors, mission planning workstations, engineering dashboards, CI/CD runners, Ground Station antenna control systems, signal conditioning management interfaces, launch sequencing processors, launch monitoring consoles, Facility Management PLC engineering workstations, network management hosts, GaaS administrative portals, and security operations infrastructure. Multi-factor authentication (MFA) shall be required for privileged roles, mission operators, launch personnel, network administrators, cryptographic custodians, and security platform administrators. Shared, default, or vendor-provided accounts on OT devices, PLCs, SCADA systems, antenna control units (ACUs), SDR controllers, RF switch controllers, amplifier management interfaces, and relay controllers shall be eliminated or disabled wherever technically feasible. Where device-level identity enforcement is supported, individual named accounts shall replace generic logins to preserve accountability. For legacy OT controllers and embedded systems that cannot natively enforce modern authentication, access shall be restricted through hardened jump hosts or controlled engineering consoles that enforce MFA prior to session establishment. Centralized identity services shall manage authentication across mission consoles, servers, network devices, and administrative systems to ensure consistent credential lifecycle control, including onboarding, role changes, and revocation. Strong authentication shall also be applied to infrastructure enforcement points, including VPN concentrators, firewalls, routers, switches, DNS/DHCP management systems, storage consoles, and management networks, to prevent credential-based takeover of mission network control planes. Service accounts shall be segregated from user identities, assigned least-privilege permissions, and managed using secure credential storage mechanisms. Regular account audits shall identify orphaned, dormant, or over-privileged accounts, with heightened review cycles during mission-critical phases such as launch campaigns, maneuver execution periods, or high-risk operational transitions. Personnel shall be trained on credential hygiene, social engineering awareness, secure token handling, and protection of hardware authenticators. At this level, endpoint authentication reduces the likelihood of unauthorized access resulting from stolen credentials, brute-force attempts, default account misuse, remote service abuse, or weak administrative practices across Ground Station, Mission Operations, Launch, Networking, GaaS, and Security Operations environments.	Endpoint authentication shall align with Zero Trust identity principles and incorporate continuous validation of user, device, service, and contextual posture prior to granting and maintaining access. Authentication decisions shall evaluate device health, network origin, mission phase, behavioral risk indicators, and role sensitivity to dynamically assess trust and restrict access during elevated-risk operational windows. Certificate-based or hardware-token-backed authentication shall be required for OT engineering accounts, mission administrators, launch control personnel, network infrastructure administrators, cryptographic key custodians, GaaS control-plane operators, and security platform administrators. Hardware roots of trust and secure credential storage mechanisms shall be used where supported to prevent credential extraction from endpoints, including engineering consoles and administrative workstations. Mutual cryptographic authentication shall be enforced for service-to-service communications between command systems, telemetry pipelines, scheduling engines, backend databases, CI/CD tooling, and automation frameworks to prevent impersonation or token replay. Authentication controls shall extend to Ground Station antenna control APIs, SDR configuration interfaces, RF routing systems, launch sequencing processors, monitoring dashboards, Facility Management PLC interfaces, and GaaS command gateways to prevent unauthorized logic modification, relay reconfiguration, or safety-critical state manipulation. Conditional access controls shall dynamically restrict authentication for high-impact roles during launch campaigns, fueling operations, or other critical mission phases. Dual-operator authentication workflows shall be required for safety-critical actions such as modification of launch sequencing parameters, abort logic updates, fueling valve activation, RF path reconfiguration, cryptographic key rotation, or firmware promotion into operational environments. Authentication telemetry shall feed directly into SOC and DCO monitoring pipelines, enabling detection of anomalous patterns such as off-hours access, geographically inconsistent logins, device fingerprint mismatches, rapid privilege escalation, or abnormal service-account usage. Red-team adversary emulation shall validate resilience against credential theft, brute force, token replay, session hijacking, service account abuse, federated identity misuse, and authentication bypass attempts across both IT and OT environments. Validation shall include testing of GaaS authentication boundaries, network device management planes, cryptographic systems, and security operations platforms. At this level, endpoint authentication operates as a continuously validated identity assurance and lateral-movement containment mechanism, preventing unauthorized user, process, or device access to mission-critical endpoints and constraining adversary pivoting across Ground Station, Mission Operations, Launch Systems, Networking Infrastructure, GaaS control planes, and Security Operations environments during high-impact mission phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-4	Malicious code protection shall be deployed across all supported IT endpoints and mission-support systems, including Mission Operations Center command and control servers, telemetry ingestion and processing hosts, mission planning workstations, engineering dashboards, Ground Station antenna control systems, RF management interfaces, launch sequencing servers, launch monitoring platforms, CI/CD runners, GaaS command gateways, and security operations infrastructure. Anti-virus and anti-malware agents shall provide both signature-based and behavioral detection capabilities and shall automatically update from trusted repositories to maintain protection against emerging threats. Endpoint defenses shall remain continuously active and monitor for malicious behaviors like scripting abuse, unauthorized process spawning, persistence mechanisms, obfuscation attempts, misuse of command interpreters, privilege escalation attempts, and living-off-the-land techniques. Processing and archive servers shall be specifically monitored for ransomware-related behaviors that could impact mission data availability, including unauthorized encryption or destructive modification of telemetry, command artifacts, ephemeris files, configuration data, and historical mission archives. Engineering workstations, telemetry processors, dashboard hosts, CI/CD systems, and integration testing platforms shall be monitored for malicious script execution, unauthorized binary introduction, and modification of system processes. Launch control systems and monitoring consoles shall maintain active endpoint protections to detect malicious activity during time-constrained launch windows where manual response time is limited. For OT and ICS devices where endpoint agents cannot be installed, including PLC controllers, antenna servo systems, fueling infrastructure, and facility management components, protections shall be implemented through hardened jump hosts, strict network segmentation, and monitoring of command traffic to detect anomalous execution patterns or malware indicators. Removable media shall be scanned prior to use on mission consoles, engineering systems, or launch infrastructure, or alternatively blocked outright where operationally feasible. Malware alerts and behavioral detections shall be logged and forwarded to the Security Operations Center for review and correlation. Operators shall be trained not to disable or bypass endpoint protections during mission-critical operations. At this level, malicious code protection reduces exposure to scripting abuse, runtime manipulation, unauthorized persistence, ransomware activity, and denial-of-service conditions that could degrade mission availability across Ground Station, Mission Operations, Launch, Networking, GaaS, and Security Operations functions.	Malicious code protection shall operate as a real-time, telemetry-integrated detection and containment capability spanning IT systems, engineering environments, CI/CD pipelines, launch infrastructure, networking platforms, GaaS control planes, and mission-critical OT interfaces. Endpoint Detection and Response (EDR) platforms shall be required on all supported systems and shall provide continuous behavioral analytics, memory inspection, process lineage tracking, credential access monitoring, and detection of living-off-the-land techniques, obfuscated tooling, and unauthorized persistence mechanisms. EDR telemetry shall integrate directly into SOC and DCO pipelines for automated correlation with authentication, network, file integrity, and telemetry events. Detection coverage shall extend to command sequencing stacks, telemetry processing pipelines, orbital planning tools, engineering analytics platforms, Ground Station control interfaces, launch control processors, and security service hosts to ensure that malware or unauthorized code cannot compromise authoritative mission logic. Suspicious files, scripts, firmware updates, CI/CD artifacts, and integration test payloads shall undergo sandbox detonation and behavioral analysis prior to promotion into operational mission networks or launch environments. Engineering toolchains, automation systems, GaaS processing components, and IR toolkits shall be monitored for storage of malicious payloads, staged implants, and unauthorized scripting execution. Removable media shall be strictly controlled using hardware-based or policy-enforced whitelisting mechanisms, and unapproved devices shall be automatically blocked. For OT consoles, launch systems, and facility management interfaces, adaptive containment mechanisms shall automatically isolate affected endpoints upon detection of malicious behavior while preserving safe-state transitions and safety interlocks to avoid unintended physical consequences. Detection logic shall explicitly include ransomware behaviors, data destruction attempts, firmware tampering, malicious update delivery, service stoppage conditions, and ICS-specific malware patterns targeting PLC logic, relay firmware, or control-state manipulation. Protections shall extend to security monitoring stacks, deception environments, and DCO infrastructure to prevent adversaries from implanting malware within defensive tooling. Adversary emulation and red-team exercises shall validate that injected payloads, unauthorized scripts, malicious firmware, and supply-chain-delivered implants are detected and contained under realistic operational conditions, including constrained launch windows where response must be automated. At this level, malicious code protection functions as an active mission assurance control that detects, correlates, and contains advanced malware, ransomware, obfuscated payloads, persistence techniques, and ICS-targeted attacks before they can impact mission command integrity, telemetry accuracy, engineering workflows, launch sequencing, facility safety systems, or ground infrastructure resilience.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-5	Recoverable backups shall be maintained for all endpoint and control systems supporting Ground Station, Mission Operations, Launch, Networking, GaaS, and Security Operations functions. Backup scope shall include Mission Operations command sequencing systems, telemetry processors, orbital planning tools, engineering workstations, command dictionaries, mission history archives, science data repositories, configuration repositories, CI/CD artifacts, network device configurations, SIEM rule sets, identity management policies, and security tooling configurations. For Ground Station systems, backups shall include antenna control configurations, RF routing parameters, DSP profiles, calibration states, and management server configurations. For Launch environments, backups shall include sequencing applications, abort logic definitions, monitoring dashboards, integration testing artifacts, and critical control system configurations. Backups shall be performed on a schedule commensurate with mission criticality and retained in protected storage logically separated from production environments to prevent compromise through ransomware, destructive malware, or lateral movement. Authoritative telemetry archives, anomaly baselines, trend datasets, mission planning artifacts, and test validation records shall be included to enable reconstruction following data manipulation or service disruption events. Access to backup repositories shall be restricted, monitored, and logged to prevent unauthorized deletion, modification, or tampering. Restoration testing shall be conducted periodically to validate that backups are complete, consistent, and capable of restoring mission-critical systems within defined recovery objectives. During mission-critical windows such as launch campaigns, maneuver execution periods, or high-risk operational phases, backup currency and restoration readiness shall be explicitly verified. At this level, backups provide foundational resilience against ransomware, data destruction, configuration corruption, manipulation of authoritative mission artifacts, and denial-of-service conditions affecting command systems, telemetry history, engineering data, or launch infrastructure.	Backup mechanisms shall be hardened, isolated, cryptographically protected, and validated as part of mission assurance strategy. Backup systems shall implement immutable storage controls, including write-once or version-locked retention mechanisms, preventing modification or deletion of protected recovery points. Backup repositories shall be logically and physically segmented from operational networks, including separation from identity providers and administrative domains, to resist adversary access following credential compromise or privilege escalation. Mission-critical components shall have explicitly defined recovery priorities and restoration playbooks aligned to operational impact. These components shall include launch sequencing systems, abort logic definitions, PLC configuration states, antenna control baselines, RF path routing tables, DSP firmware, command dictionaries, telemetry baselines, orbital planning models, cryptographic firmware and configuration states, key management system configurations, SIEM rules, DCO playbooks, identity management policies, and GaaS scheduling and gateway configurations. Offline or air-gapped backup copies shall be maintained for high-value systems to prevent coordinated destruction of both production and backup environments. Backup validation shall include cryptographic integrity verification of backup images, configuration states, and firmware artifacts prior to restoration. Continuous monitoring shall verify backup job success, detect unauthorized access to backup storage, and generate alerts on abnormal deletion attempts or retention policy changes. Recovery procedures shall ensure that restoration of OT systems, launch control logic, or RF management configurations does not introduce unsafe states or bypass required safety interlocks. Adversary emulation and destructive attack simulations shall test ransomware, data destruction, indicator removal, and coordinated denial-of-service scenarios to validate that recovery operations can be executed under time-constrained conditions such as launch windows or emergency maneuver situations. Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) shall be formally defined, documented, and exercised to ensure that restoration of command, telemetry, engineering, networking, and security systems can occur without cascading operational disruption. At this level, backups operate as a mission continuity and integrity assurance mechanism, ensuring rapid restoration of authoritative configuration state, control logic, telemetry history, cryptographic baselines, and defensive tooling even in the presence of destructive malware, insider misuse, supply chain compromise, or coordinated attack during high-impact mission phases.

END-6	An authoritative inventory shall be maintained for all physical mission systems and devices, such as servers, workstations, network equipment, RF hardware, ground station control systems, PLCs, launch infrastructure components, and removable media Secure configuration baselines shall be established, documented, and enforced across all mission endpoints supporting Ground Station, Mission Operations, Launch, Networking, GaaS, and Security Operations functions. For IT systems, industry-recognized hardening standards such as CIS Benchmarks or STIGs shall be applied to mission servers, operator consoles, telemetry processors, dashboard systems, CI/CD runners, archive servers, storage platforms, and management hosts. Baselines shall disable unnecessary services, enforce secure authentication settings, restrict administrative privileges, and harden configurations against common exploitation paths. For Ground Station systems, known-good configurations shall be maintained for antenna control units (ACUs), servo controllers, tracking servers, calibration systems, RF switching systems, amplifiers, signal path controllers, hopping tables, nulling profiles, DSP modes, and associated management interfaces to prevent unauthorized modification of control behavior, attenuation parameters, or firmware states. For Mission Operations systems, baseline enforcement shall protect command sequencing servers, command and telemetry dictionaries, scheduling and planning systems, anomaly detection thresholds, decoder configurations, science processors, and archive services from unauthorized modification or silent drift. For Launch and Facility Management systems, vendor-provided hardening guidance shall be applied to PLCs, HMIs, SCADA components, relay processors, transceiver software, launch sequencing systems, abort logic modules, visualization platforms, and test harnesses. Configuration settings shall be documented and reviewed prior to mission-critical operations to prevent unauthorized modification of safety logic, abort parameters, or control tasking. For Networking and Management Services, known-good baselines shall be maintained for routers, switches, firewalls, crypto appliances, DNS/DHCP servers, time services, management controllers, PXE servers, storage services, and provisioning hosts to prevent unauthorized changes to ACLs, routing tables, recursion settings, protocol handlers, snapshot policies, or authentication mechanisms. Configuration validation shall be automated where feasible to reduce manual drift. A centralized repository of approved configuration states shall serve as the authoritative reference for comparison prior to operational use, particularly before launch campaigns or high-impact mission phases. Personnel shall be trained to recognize signs of configuration drift, weakened security settings, unauthorized service enablement, or suspicious changes to safety-critical parameters. At this level, configuration control reduces exposure to misconfiguration, unauthorized modification, insecure defaults, silent defense impairment, and degradation of mission integrity across command, telemetry, networking, OT, and launch systems.	For the physical inventory, the inventory shall record device identifier, type, location, owner, custodian, mission function, firmware/software version, and lifecycle state. Asset inventory shall be continuously updated using automated discovery and reconciliation tools. Unauthorized, untracked, or rogue devices shall trigger investigation and removal procedures. Configuration control shall enforce cryptographically validated, continuously monitored, and, where feasible, immutable endpoint states across IT and OT systems. IT infrastructure shall adopt immutable or declarative deployment models where practical, with systems rebuilt from version-controlled configuration definitions rather than modified in place. Firmware images, configuration templates, trust stores, security policies, hopping profiles, RF routing tables, launch abort definitions, and mission-critical software settings shall require cryptographic signing and validation at boot or load time to prevent unauthorized modification. Real-time drift detection mechanisms shall continuously monitor mission servers, Ground Station control systems, OT devices, networking infrastructure, SOC tooling, GaaS gateways, and identity systems for deviations from approved baselines. Drift detection shall include monitoring of service enablement, privilege assignments, firmware versions, DSP modes, crypto settings, routing configurations, logging states, anomaly thresholds, visualization filters, and safety-critical parameters. Unexplained drift shall trigger alerting, investigation, and formal approval prior to continued operational or launch progression. Cryptographic attestation mechanisms shall validate endpoint integrity, including boot state, firmware hash, configuration hash, and security enforcement state. Upon detection of unauthorized changes, automated containment, rollback to known-good baselines, or mission hold procedures shall be initiated in accordance with operational safety constraints. Drift telemetry shall feed directly into SOC and DCO monitoring pipelines for correlation with authentication anomalies, logging suppression attempts, physical state transitions, and adversary-informed threat indicators. Strict baseline enforcement shall extend to defensive infrastructure, including IDS/IPS platforms, EDR systems, SIEM pipelines, SOAR playbooks, deception hosts, IR workstations, forensic servers, and vulnerability scanners, ensuring that attackers cannot silently impair defenses or weaken monitoring through configuration manipulation. Baseline enforcement on DNS/DHCP, network devices, crypto appliances, and management-plane controllers shall prevent unauthorized modification of traffic handling, encryption parameters, trust relationships, or identity enforcement mechanisms. Adversary emulation exercises shall validate that drift detection and attestation mechanisms detect or prevent exploit paths such as unauthorized service enablement, modification of authentication processes, privilege escalation configuration changes, trust store alteration, disabled logging agents, weakened cryptographic settings, altered PLC logic, modified abort parameters, or silent safety interlock manipulation. At this level, endpoint configuration control functions as a continuous mission integrity enforcement mechanism, ensuring all mission systems remain in a cryptographically verified, known-good state and preventing silent degradation of security posture or safety logic prior to or during high-impact mission and launch operations.

END-7	Separation of duties shall be enforced across all mission, ground station, launch, networking, security operations, and Ground Station-as-a-Service (GaaS) endpoints to ensure that no single user, account, or system role has complete authority over critical mission functions. Operators and administrators shall maintain separate accounts, with administrative privileges restricted to dedicated accounts that are not used for routine operational activities. Role-Based Access Control (RBAC) policies shall ensure that mission operators cannot administer mission servers, modify system baselines, alter security configurations, or adjust cryptographic material outside their defined operational scope. Within Ground Station environments, RF defense operators, maintenance personnel responsible for firmware and patch management, and approval authorities for configuration changes shall be distinct roles. A single individual shall not be able to both modify RF logic (e.g., hop tables, nulling profiles, gain settings) and suppress associated logging or monitoring artifacts. Within Mission Operations, duties related to command authoring, command approval, command upload, and execution shall be separated to prevent unilateral issuance of high-impact spacecraft commands. In Launch and Facility Management environments, engineering workstations used for configuration changes, PLC programming, abort logic updates, or fueling system adjustments shall be logically and operationally separated from Human Machine Interface (HMI) consoles used for routine monitoring and operational control. Individuals responsible for sequencing logic shall not also control safety overrides or monitoring dashboards. For Networking and Security Services, network administration, cryptographic/key management, identity administration, logging administration, patch management, and monitoring system configuration shall be distinct roles. No single account shall be capable of modifying routing enforcement, altering identity policy, adjusting log retention, and suppressing detection controls simultaneously. Within GaaS environments, scheduling request roles, schedule approval roles, API administration, credential issuance, and subscription/billing administration shall be separated to prevent single-account dominance over contact allocation and service enforcement. Role assignments shall be reviewed at defined intervals, with heightened review during mission-critical periods such as launch campaigns. Service accounts shall be constrained to narrowly defined tasks and shall not possess interactive administrative privileges. Personnel shall be trained on least-privilege principles and the operational importance of role separation. At this level, separation of duties reduces blast radius by ensuring that compromise of a single identity cannot immediately result in full administrative, operational, cryptographic, scheduling, or safety control of mission systems.	Separation of duties shall be enforced through infrastructure-backed isolation mechanisms and time-bound privilege controls to prevent role convergence across IT, OT, launch, networking, SOC, and GaaS domains. Administrative and operational functions shall execute on physically separate endpoints or strongly isolated virtual environments with strict boundary enforcement. Privileged administrative access shall be provisioned using JIT elevation mechanisms and automatically revoked upon task completion. Privilege elevation workflows shall require explicit approval and shall be tightly time-bound, particularly during mission-critical phases such as launch campaigns, fueling sequences, abort readiness states, high-value contact windows, cryptographic key rotations, or command loads. Dual-approval or multi-party authorization shall be required for actions affecting safety-critical systems, launch sequencing logic, PLC configuration states, cryptographic material generation or deployment, schedule allocation overrides, firmware promotion, or detection pipeline modification. In Ground Station environments, RF control authority, firmware management, and monitoring configuration authority shall be enforced on separate systems or enclaves. In Mission Operations, individuals capable of authoring commands shall not be capable of independently approving, uploading, and executing those commands without secondary validation. In Launch systems, individuals responsible for abort logic updates shall not also administer logging pipelines or safety monitoring systems. For Networking and Security Operations, roles responsible for identity policy, certificate issuance, routing enforcement, SIEM administration, detection engineering, playbook orchestration, and red/purple team tooling shall not converge into a single operational identity. Detection engineering, threat intelligence ingestion, and automated response control shall be separated to prevent unilateral impairment of defensive capabilities. Within GaaS environments, identity administration, token issuance, key management, scheduling approval, subscription tier modification, and audit review shall be structurally separated. No single compromised account shall be capable of issuing credentials, validating access, modifying schedule priority, and erasing audit trails end-to-end. Continuous monitoring shall detect cross-role activity, privilege escalation attempts, and anomalous combinations of access across mission domains. SOC systems shall correlate administrative logins with operational events such as unexpected PLC access during countdown, abnormal RF parameter changes, unauthorized schedule reallocation, or cryptographic key export operations. Red-team adversary emulation shall validate that privilege escalation paths, credential reuse across roles, and administrative bypass attempts are detected and constrained. Testing shall specifically validate that no single compromised account can both execute mission-impacting changes and suppress the associated logging, detection, or audit mechanisms. At this level, separation of duties functions as a structural mission containment mechanism that prevents

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
		unilateral authority over systems, ensuring that no single compromised identity or malicious insider can independently subvert mission safety, availability, or integrity during high-impact operational phases.
END-8	Endpoint Data Loss Prevention (DLP) controls shall monitor and regulate handling of sensitive mission data on operator workstations, engineering consoles, mission servers, CI/CD runners, and other endpoint devices that store or process mission artifacts. Endpoint DLP shall inspect file transfers, removable media usage, clipboard operations, email attachments, file uploads, and API-based data movement to detect unauthorized or high-risk data transfer activity. Policies shall be configured to identify and classify mission-specific sensitive data types, including command files, command dictionaries, execution history logs, orbital models, telemetry archives, firmware artifacts, configuration baselines, CI/CD secrets, API tokens, and cryptographic material. DLP controls shall detect bulk reads, abnormal file staging, compression of sensitive directories, and attempts to export protected datasets over network channels, removable media, or external collaboration tools. Suspected exfiltration attempts shall be blocked where technically feasible or generate alerts for investigation. All DLP events shall be logged and forwarded to centralized monitoring systems to support correlation with authentication logs, network activity, and endpoint telemetry. Periodic review of DLP alerts shall be conducted to identify risky behavior patterns, misconfigurations, excessive data access, or potential insider misuse. Personnel shall receive training on proper handling of sensitive mission data and procedures for reporting accidental or suspicious data transfer attempts. At this level, endpoint DLP reduces the likelihood of inadvertent data leakage, credential exposure, and opportunistic exfiltration of mission-critical artifacts, while providing visibility into endpoint-level attempts to export sensitive command, telemetry, or configuration data.	Endpoint DLP shall operate with adaptive, context-aware enforcement policies that evaluate user role, device posture, mission phase, data classification, and behavioral patterns prior to permitting sensitive data transfer. Mission-critical datasets shall be fingerprinted, cryptographically identified, or content-matched to enable real-time detection and blocking of unauthorized copying, compression, encryption, staging, or export attempts. Highly sensitive artifacts, including cryptographic keys, trust stores, launch sequencing materials, command authority files, scheduling priority configurations, and authoritative telemetry baselines, shall require multi-party approval workflows prior to export. Export restrictions shall dynamically tighten during mission-critical phases such as launch preparation, fueling operations, contact windows, or high-priority mission events. Endpoint DLP telemetry shall be streamed to SOC pipelines and correlated with authentication events, privilege elevation activity, network flows, removable media insertion, and abnormal user behavior patterns. Integration with insider threat monitoring programs shall enable detection of bulk data staging, anomalous after-hours access, abnormal archive downloads, or attempts to bypass policy through alternate channels. USB device control shall enforce strict whitelisting, with automatic blocking of unapproved removable media, particularly on engineering workstations, launch consoles, cryptographic management systems, and CI/CD environments. Attempts to copy credential stores, environment files, token dumps, or configuration artifacts shall generate high-priority alerts. Adversary emulation exercises shall simulate insider-driven and credential-abuse exfiltration scenarios, including unauthorized USB insertion during launch preparation, bulk download of mission archives, staged compression of telemetry history, export of cryptographic material, or transfer of CI/CD secrets to external systems. Controls shall be validated to ensure that such attempts are blocked or detected with actionable fidelity. At this level, endpoint DLP functions as a high-assurance containment mechanism that prevents mission-critical data, credentials, cryptographic material, and authoritative command artifacts from leaving controlled endpoints without authorization, significantly reducing insider threat impact and constraining adversary exfiltration pathways during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-9	File Integrity Monitoring (FIM) shall be deployed on mission-critical endpoints and directories to detect unauthorized modification of sensitive files, firmware images, and configuration artifacts across ground station systems, mission operations infrastructure, launch environments, networking services, and security platforms. Monitoring scope shall include command and telemetry databases, sequencing logic, abort rule definitions, orbital models, TLEs, telemetry processing configurations, science processing outputs, firmware images, RF controller configurations, PLC logic files, routing and crypto enforcement configurations, time service settings, detection rulesets, and other authoritative mission artifacts. Cryptographic hashing mechanisms shall establish approved baseline integrity states for protected files. Periodic integrity checks shall compare current file states against these baselines and generate alerts upon detection of deviations. Monitoring shall record sufficient context to identify the user, process, timestamp, and system associated with the modification, enabling reconstruction of manipulation attempts affecting command systems, telemetry products, control logic, network enforcement points, or security monitoring infrastructure. Integrity monitoring shall extend to firmware repositories, PXE and provisioning directories, CI/CD artifacts, key stores, certificate chains, and crypto libraries to detect unauthorized replacement, insertion, or weakening of trusted components. File changes associated with antenna control behavior, RF signal routing, launch sequencing modules, anomaly detection thresholds, controller tasking logic, or dashboard visualization assets shall be treated as high-priority events due to potential mission or safety impact. All integrity violation alerts shall be forwarded to centralized logging or SIEM platforms for correlation with authentication events, privilege escalations, configuration changes, and OT telemetry. Personnel shall be trained to escalate integrity failures immediately, particularly during launch campaigns, command loads, contact windows, or other mission-critical phases. At this level, file integrity monitoring provides early detection of unauthorized tampering, stored data manipulation, configuration drift, firmware replacement, and silent weakening of security controls that could compromise mission operations or degrade launch safety.	File integrity enforcement shall be cryptographically enforced, continuously validated, and tightly integrated into automated containment and recovery workflows. All mission-critical files, including launch sequencing logic, abort parameters, fueling thresholds, command dictionaries, telemetry transformation pipelines, RF control firmware, PLC configurations, network device policies, time synchronization settings, detection rulesets, and cryptographic materials, shall require cryptographic signing prior to operational promotion or activation. Systems shall verify digital signatures at load time and, where feasible, during runtime to ensure only authorized and trusted artifacts are executed. Continuous integrity monitoring tools shall perform real-time validation of protected files and firmware across IT, OT, and security infrastructure. Unauthorized or unapproved modifications shall trigger automated response actions, including rollback to last known-good versions, quarantine or isolation of affected endpoints, suspension of sequencing or automation workflows, and escalation to incident response teams. Integrity telemetry shall be correlated with authentication logs, privilege elevation events, network configuration changes, anti-jam algorithm modifications, relay firmware updates, time service adjustments, and SOC rule alterations to detect coordinated multi-layer tampering. During mission-critical windows such as launch operations, changes to sequencing logic, abort modules, crypto material, RF control parameters, or controller firmware shall require dual approval prior to commit or activation. Integrity controls shall extend to detection platforms themselves, including IDS/IPS rules, SIEM parsers, log forwarder configurations, deception triggers, forensic tools, and SOAR playbooks, ensuring that adversaries cannot silently impair defenses without detection. Monitoring of time-service configurations shall detect attempts to manipulate timestamps or synchronization behavior intended to obscure attacker activity. Adversary emulation shall validate that integrity monitoring detects stealthy and incremental manipulation, insertion of backdoored firmware, alteration of routing policies, corruption of telemetry baselines, poisoning of detection content, modification of controller tasking logic, or replacement of trusted binaries in provisioning repositories. At this level, file integrity monitoring functions as a cross-domain mission integrity preservation mechanism, ensuring that silent or incremental tampering of control logic, firmware, telemetry products, network enforcement points, security tooling, or cryptographic components cannot occur without immediate detection, correlation, and enforced recovery actions during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-10	Host-based firewalls shall be enabled and properly configured on all supported mission endpoints, including Mission Operations Center security systems, command and control servers, telemetry processors, planning and orbit determination servers, engineering workstations, launch sequencing systems, OT controllers, and supporting infrastructure services. Firewalls shall enforce a default-deny inbound posture, permitting only explicitly authorized ports, protocols, and services required for the endpoint's defined operational role. Rules shall be tailored to isolate mission enclaves from enterprise IT networks, payload development labs, partner environments, and external services. Command and control stacks, launch control processors, anti-jam management interfaces, relay controllers, RF management systems, and telemetry databases shall not rely solely on perimeter firewalls but shall enforce host-level restrictions to reduce exposure to remote service exploitation, man-in-the-middle staging, and lateral pivoting attempts. High-risk administrative and lateral movement services, including SSH, SMB, WinRM, WMI, RDP, and similar protocols, shall be disabled or restricted unless explicitly required for mission operations. Planning servers, orbit determination systems, scheduling platforms, and launch stacks shall permit only required communications to approved peer systems. All blocked inbound and outbound connection attempts shall be logged and forwarded to centralized monitoring platforms. Outbound filtering shall be implemented where operationally feasible, particularly on OT endpoints, launch infrastructure, telemetry processors, and cryptographic service hosts, to prevent unauthorized external communications, command-and-control beaconing, or data exfiltration attempts. Firewall configurations shall be reviewed and validated prior to mission-critical phases, including launch campaigns, to ensure temporary rules have not expanded beyond operational necessity. At this level, host firewalls enforce device-level network least privilege, isolate mission systems from enterprise and external exposure, and reduce the risk of lateral movement and remote exploitation across ground, launch, and operational environments.	Host firewalls shall implement application-aware, identity-aware, and Zero Trust-aligned enforcement policies that provide endpoint-level micro-segmentation across mission infrastructure. Enforcement shall restrict communications not only by port and protocol, but also by authorized process, service identity, authenticated role, and defined trust boundary. Distinct, role-specific firewall policies shall be enforced for operator consoles, command sequencing servers, telemetry processors, orbit determination systems, anti-jam management interfaces, launch control processors, OT PLC controllers, relay systems, and cryptographic appliances. Each endpoint shall be permitted to communicate only with explicitly authorized systems necessary for its mission function, preventing cross-functional lateral movement between security services, C2 stacks, launch systems, and facility management infrastructure. Firewall policies shall restrict communications between enterprise IT and mission enclaves, ensuring that compromise of enterprise or partner systems cannot directly pivot into command, telemetry, or launch control environments. Host-level enforcement shall constrain management-plane access on middleware nodes, routers, crypto appliances, and network service hosts to prevent unauthorized protocol abuse, MITM staging, or remote service exploitation. Firewall telemetry shall stream continuously into SOC pipelines for correlation with authentication anomalies, file integrity alerts, configuration drift detections, and endpoint behavioral monitoring. Adaptive response mechanisms shall automatically isolate endpoints exhibiting suspicious behaviors such as lateral scanning, unauthorized attempts to access fueling controllers, relay processors, antenna control systems, cryptographic services, or telemetry archives. Geo-based restrictions, network reputation filtering, and contextual outbound controls shall be implemented where operationally appropriate to reduce exposure to anomalous external communications during high-impact mission phases. During launch campaigns or other mission-critical windows, firewall rule modifications shall require controlled change management and formal approval workflows. Adversary emulation exercises shall validate that host firewall policies prevent lateral movement, privilege pivoting, remote service exploitation, and unauthorized network access to high-value systems, including launch sequencing logic, fueling infrastructure, antenna controllers, cryptographic management systems, and telemetry processing nodes. At this level, host firewalls function as endpoint-enforced micro-segmentation controls that structurally isolate mission enclaves, constrain adversary pivot paths, and preserve command, telemetry, and launch integrity even in the presence of compromised credentials or adjacent system breaches.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-11	Endpoint hardening baselines shall be applied across all mission IT and OT endpoints, including antenna control systems, tracking servers, RF controllers, Mission Operations Center servers, command and control stacks, telemetry processors, engineering workstations, launch sequencing systems, monitoring platforms, storage appliances, time servers, SOC infrastructure, DCO/IR platforms, and supporting network management systems. Recognized hardening standards such as CIS Benchmarks and DISA STIGs shall be implemented on IT systems to reduce attack surface and enforce secure configuration settings. Unnecessary services, debug interfaces, legacy protocols, and exposed management ports including Telnet, FTP, legacy SNMP, unsecured remote administration services, unused SSH endpoints, and non-essential WMI/WinRM interfaces shall be disabled unless explicitly required for mission function. Services retained for operational necessity shall be hardened through secure configuration, restricted administrative access, encrypted management protocols (e.g., HTTPS, SSH with key-based authentication + passphrase), and least-privilege service accounts. For OT and launch-related systems (e.g., PLCs, HMIs, relay processors, antenna control units, RF path controllers, fueling systems, and supervisory infrastructure) vendor hardening guidance shall be followed to remove default accounts, disable unused control ports, restrict firmware update paths, disable maintenance modes outside approved windows, and limit exposed engineering features that could enable unauthorized control or code execution. Security monitoring platforms, DCO tools, IR workstations, deception systems, storage systems, and time services shall also be hardened to remove unnecessary services and administrative interfaces, reducing exploitability of defensive infrastructure itself. Hardening shall be validated through periodic automated scans and manual configuration reviews, particularly prior to mission-critical operations such as launch campaigns. Administrators shall be trained to recognize insecure defaults, unnecessary service exposure, and high-risk configuration states. At this level, endpoint hardening reduces attack surface, removes opportunistic exploitation pathways, and limits remote service abuse, living-off-the-land execution, denial-of-service risk, and unauthorized control of mission and launch systems.	Endpoint hardening shall be enforced as a cryptographically validated, continuously monitored security posture across mission IT, OT, launch, networking, and SOC infrastructure. All supported endpoints shall implement secure boot mechanisms with cryptographic firmware signing and validation to prevent unauthorized firmware modification, bootkits, or insertion of malicious low-level components. Mission systems shall utilize hardened, version-controlled “gold images” for servers, engineering workstations, launch processors, telemetry systems, monitoring platforms, DCO/IR tooling, and management hosts. These images shall be rebuilt and revalidated prior to mission-critical windows to eliminate configuration drift and reduce residual exposure from prior operational cycles. Continuous monitoring mechanisms shall detect unauthorized activation of services, re-enablement of debug interfaces, modification of management settings, or reintroduction of insecure protocols. Detected deviations from approved hardened baselines shall trigger containment or reversion to known-good states. Hardened configurations shall include minimization of administrative tooling capable of living-off-the-land abuse, removal of unused interpreters or scripting engines where feasible, restriction of system utilities that enable remote exploitation, and lockdown of exposed APIs or web-based administrative portals. Hardening compliance shall be tied directly into mission readiness checks, preventing systems from progressing into launch campaigns, high-tempo operational windows, or critical mission phases without verified secure posture. Device attestation mechanisms, such as TPM-backed validation or equivalent hardware-rooted trust mechanisms, shall be used to verify endpoint state integrity before allowing operational participation. Hardening controls shall extend to network infrastructure devices, storage systems, time servers, SOC platforms, deception assets, and GaaS management systems, ensuring that enforcement points, routing logic, detection engines, and orchestration platforms cannot be easily exploited or repurposed by adversaries. Red-team and adversary emulation exercises shall validate that hardened endpoints resist exploitation techniques such as remote service abuse, privilege escalation, ICS malware insertion, defense impairment, denial-of-service preparation, and manipulation of monitoring or orchestration systems. At this level, endpoint hardening functions as a proactive attack-surface minimization and resilience mechanism, ensuring that mission-critical systems operate with only necessary services exposed, are cryptographically anchored to known-good states, and maintain resistance to exploitation across ground, launch, and operational mission environments.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-12	Host-based intrusion detection and prevention capabilities shall be deployed on all supported IT mission endpoints, including mission servers, operator consoles, telemetry processors, mission management systems, planning and scheduling servers, engineering workstations, dashboard systems, storage servers, CI/CD runners, and supporting infrastructure hosts. HIDS/HIPS agents shall monitor system logs, file integrity, registry or configuration changes, process creation events, service modifications, and suspicious behavioral patterns indicative of exploitation or post-compromise activity. Prevention rules shall be configured to block common exploit techniques (e.g., buffer overflows, code injection, privilege escalation attempts, unauthorized service creation, registry modification, and suspicious scripting activity). Policies shall be tuned to mission-specific environments to reduce false positives while maintaining detection fidelity, recognizing that legitimate activities such as telemetry parser updates, orbital model recalculations, or deployment of mission scripts may otherwise resemble exploit behavior. Mission management servers, orbital propagation engines, scheduling systems, and command authoring platforms shall be specifically monitored for scripting abuse, unauthorized logic modification, or manipulation attempts affecting authoritative mission data. Engineering consoles, CI/CD systems, and dashboard platforms shall be monitored for persistence mechanisms, abnormal process spawning, or modification of trusted binaries. For OT and launch-related devices that cannot support native host agents, equivalent monitoring shall be implemented at hardened jump hosts, hypervisors, or adjacent management layers to detect suspicious command execution patterns, abnormal service behavior, or attempts to manipulate control logic. All host-based alerts shall be forwarded to centralized SIEM or SOC platforms for correlation and response. At this level, HIDS/HIPS provides localized detection and exploit blocking, reducing risk from remote service abuse, scripting-based attacks, privilege escalation, defense impairment, and tampering across mission and launch infrastructure.	Host-based intrusion detection and prevention shall evolve into a behaviorally driven, autonomous containment capability tightly integrated with enterprise SOC fusion and mission telemetry analysis. Advanced Endpoint Detection and Response (EDR) platforms shall be required on all supported IT and mission-critical endpoints, providing continuous behavioral analytics, memory inspection, process lineage tracking, kernel-level monitoring, registry integrity validation, and detection of living-off-the-land techniques. Detection logic shall extend beyond signature-based controls to identify advanced techniques like defense impairment attempts, log suppression, registry tampering, credential abuse, persistence installation, and stealth process injection. Host telemetry shall stream in real time to SOC fusion dashboards where it is correlated with authentication events, network telemetry, file integrity alerts, configuration drift, and physical OT state data. Autonomous containment mechanisms shall be enforced for high-risk conditions. For example, if abnormal memory injection or unauthorized process spawning is detected on an engineering workstation or HMI during launch operations, the affected endpoint shall be automatically isolated from OT control networks while preserving safe shutdown paths and safety-critical command channels. Similarly, detection of suspicious manipulation attempts on mission management systems, scheduling engines, telemetry collectors, SIEM forwarders, or DCO infrastructure shall trigger containment workflows to prevent defense impairment or data manipulation. Monitoring shall extend to defensive infrastructure itself, including collectors, log forwarders, SIEM agents, deception hosts, forensic platforms, and IR tooling, ensuring early detection if adversaries attempt to tamper with or disable monitoring systems. Host-based controls shall include sandboxing capabilities for suspicious artifacts and high-fidelity logging of all blocked or contained actions to support forensic reconstruction and adversary pattern analysis. Adversary emulation exercises shall validate that advanced techniques such as DLL injection, unauthorized service creation, registry modification, living-off-the-land binary abuse, tampering with detection rules, or manipulation of mission-critical processes are detected and prevented under both routine and time-constrained launch-window conditions. At this level, host-based intrusion detection and prevention functions as an active mission defense mechanism that detects, correlates, and autonomously contains advanced adversary techniques before they can degrade command integrity, telemetry processing, launch safety systems, monitoring platforms, or defensive cyber operations infrastructure.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-13	Hardware- and software-based memory protection mechanisms shall be enabled across all supported mission IT endpoints, including mission servers, operator consoles, telemetry processors, mission management systems, command and control platforms, engineering workstations, CI/CD runners, security monitoring hosts, and supporting infrastructure systems. Core operating system protections such as Data Execution Prevention (DEP), Address Space Layout Randomization (ASLR), stack canaries, non-executable memory regions, and exploit guard controls shall be enforced wherever supported. Runtime memory protection mechanisms shall be applied to systems hosting security services, identity platforms, cryptographic services, and command processing logic to prevent credential extraction, in-memory key theft, token manipulation, or unauthorized modification of validation routines. Credential isolation features (e.g., LSASS protection), secure enclave protections for sensitive processes, and restricted memory access controls shall be enabled to reduce risk of credential dumping and unauthorized access token abuse. Mission command and control servers, telemetry ingestion systems, scheduling engines, orbital propagation platforms, and dashboard visualization services shall enforce memory safety protections to reduce risk of in-memory tampering with command validation logic, telemetry parsing routines, or mission-critical processing components. Compiler hardening flags shall be required for mission-developed binaries to enforce stack protection, buffer bounds checking, and memory safety enhancements. Where OT and launch systems operate on modern operating system variants (e.g., embedded Linux platforms or hardened Windows builds), kernel-level privilege separation, exploit mitigations, and secure memory handling shall be enforced. For legacy OT controllers that do not support native memory protection features, compensating controls such as hardened jump hosts, restricted execution paths, and monitoring of surrounding management systems shall be implemented. Operating system patches affecting memory management and exploit mitigations shall be tested in staging environments prior to deployment to mission-critical systems. Kernel crash logs, exploit guard triggers, and memory violation events shall be logged and forwarded to centralized monitoring platforms. Fuzz testing and structured testing of mission applications shall be conducted prior to deployment to identify unsafe memory operations. At this level, memory protection reduces the likelihood of successful exploitation of memory corruption vulnerabilities, credential extraction, in-memory manipulation of command logic, and unauthorized process injection across mission and launch infrastructure.	Memory protection shall be enforced continuously during runtime across IT, mission, launch, and supporting security systems. Advanced operating system protections such as Control Flow Guard (CFG), kernel Control Flow Integrity (kCFI), Mandatory Access Control enforcement (e.g., SELinux or AppArmor in strict enforcement mode), and signed kernel module requirements shall be mandated on supported platforms. Secure Boot and hardware-backed roots of trust shall be required to prevent unauthorized drivers, kernel modules, or low-level components from bypassing operating system memory protections. Mission-critical endpoints shall prohibit unsigned kernel extensions or memory-hooking mechanisms that could enable stealth tampering or credential harvesting. Security service hosts, identity platforms, key management systems, and HSM interface components shall enforce memory isolation to protect credentials, certificates, and cryptographic material from in-memory extraction attempts. Runtime memory events such as DEP violations, control-flow integrity failures, suspicious memory injection attempts, or anomalous kernel behavior shall stream directly into SIEM/SOC pipelines for correlation with authentication activity, file integrity alerts, network telemetry, and OT state transitions. Mission command processing systems, scheduling engines, telemetry transformation pipelines, and launch sequencing platforms shall be continuously monitored for abnormal memory behavior, including unauthorized code injection, dynamic library loading anomalies, and unexpected process memory manipulation. Endpoint detection platforms shall incorporate memory telemetry inspection to detect advanced techniques including in-memory execution, token impersonation, or stealth modification of validation logic. For OT and ICS systems, vendors shall validate that firmware and runtime components implement modern memory safety features. Where legacy systems lack native protections, hardware isolation, virtualization boundaries, or dedicated security appliances shall be used to prevent exploitation from propagating into safety-critical controllers or launch infrastructure. Mission readiness reviews shall require verification that memory protection controls are enabled, enforced, and validated across all applicable systems prior to launch campaigns or other high-impact operations. Red-team adversary emulation shall explicitly test memory corruption exploitation, credential dumping, in-memory command manipulation, and driver-level bypass attempts to validate that protections prevent or detect exploitation. At this level, memory protection functions as a hardened runtime exploitation barrier that prevents adversaries from leveraging memory corruption vulnerabilities, extracting credentials or cryptographic material, or manipulating mission-critical logic in memory during routine operations or time-constrained launch events.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-14	A formal patch management process shall be established and maintained for all mission-supporting IT endpoints, including mission servers, operator consoles, telemetry processors, command and control systems, mission management platforms, engineering workstations, CI/CD runners, security monitoring hosts, storage systems, and supporting infrastructure services. Patch inventories shall be maintained for operating systems, firmware, middleware, web services, and COTS applications. Critical security patches for IT systems shall be evaluated and applied within 30 days of release unless documented operational constraints require compensating controls. Systems supporting public-facing services, remote access pathways, scheduling APIs, web dashboards, DNS/DHCP platforms, NAS/SAN storage, SIEM interfaces, federation gateways, and network appliances shall receive prioritized patching due to elevated exposure to exploitation of remote services and public-facing applications. Patch status shall be documented and reviewed prior to mission-critical phases such as launch campaigns or major operational milestones. For OT, ICS, and launch infrastructure systems patching shall be coordinated with vendors and validated in offline staging or lab environments prior to deployment. Where patching cannot occur immediately due to mission timing, vendor constraints, or system determinism requirements, compensating controls such as network isolation, firewall restriction, or increased monitoring shall be implemented and documented. Patch freeze periods shall be formally declared during final integration and verification windows prior to launch, with strict change control to prevent destabilizing modifications. Personnel shall be trained to identify and escalate unpatched high-risk vulnerabilities, and mission leadership shall be informed of accepted risk where remediation is deferred. At this level, patch management reduces exposure to known exploited vulnerabilities across IT, mission, network, monitoring, and launch systems, limiting adversary ability to leverage public CVEs for initial access, privilege escalation, or defense evasion.	Patch management shall operate as an automated, telemetry-driven, and mission-gated enforcement mechanism across IT, OT, networking, monitoring, and launch environments. Automated patch deployment pipelines shall be implemented for IT systems, with defined maximum remediation windows such as seven days for critical vulnerabilities and fourteen to thirty days for high-severity findings unless formally waived through risk governance. Patch compliance telemetry shall feed directly into centralized dashboards and SOC monitoring platforms to provide continuous visibility into vulnerability exposure across mission systems. Systems failing to meet patch compliance thresholds shall be flagged automatically, and mission readiness gates shall prevent progression into launch or other high-impact operational phases if critical vulnerabilities remain un-remediated without documented waiver and leadership acceptance. Parallel OT and launch system testbeds shall be maintained to validate firmware updates, controller patches, and sequencing software changes prior to deployment into production environments. Firmware for ACUs, RF controllers, PLCs, crypto gateways, VPN appliances, SIEM platforms, storage arrays, DNS/IPAM systems, time services, and monitoring appliances shall undergo integrity verification and regression testing before operational use. Monitoring infrastructure, including SIEMs, IDS/IPS platforms, EDR servers, SOAR engines, and forensic systems, shall receive prioritized patching to prevent exploitation of defense tools. Network devices, crypto gateways, VPN concentrators, federation gateways, and time synchronization platforms shall be included explicitly in patch governance due to their frequent exploitation in real-world campaigns. Where emergency patching is required during active operational phases, defined emergency change control procedures shall balance risk reduction against operational stability. Compensating controls shall be formally documented when patch deployment is deferred. Adversary emulation and red-team exercises shall validate that delayed patching does not create exploitable conditions during launch windows or high-impact mission phases. Exercises shall simulate exploitation of known vulnerabilities in web services, scheduling platforms, network appliances, monitoring stacks, and OT management interfaces to ensure detection and containment mechanisms remain effective even under patch lag scenarios. At this level, patch management functions as a mission-integrated risk control that continuously reduces exploitability of known vulnerabilities, prevents exploitation of high-value infrastructure, and ties vulnerability remediation directly to mission readiness, operational authorization, and cyber risk governance.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-15	Least-privilege file permissions shall be enforced across all mission, launch, ground station, networking, and security operations endpoints. Role-Based Access Control (RBAC) shall govern read, write, execute, and delete permissions for mission servers, operator consoles, telemetry processors, launch sequencing systems, engineering workstations, storage platforms, monitoring stacks, CI/CD systems, and supporting infrastructure. Shared or generic accounts shall be eliminated in favor of named identities, and access to sensitive directories shall be granted only through formal approval workflows. Write access shall be strictly restricted for firmware images, control logic, calibration parameters, defensive configuration files, command dictionaries, command history logs, scheduling databases, orbital models, tracking inputs, telemetry archives, anomaly databases, trend stores, test artifacts, and verification scripts. Read/write separation shall be enforced between ingestion, processing, archival, and distribution roles to prevent a single compromised account from both modifying and validating authoritative mission data. File and share permissions shall be reviewed quarterly and during pre-mission readiness reviews to ensure that least-privilege policies remain aligned with operational roles. Strict access controls shall be applied to cryptographic material, token signing secrets, service configurations, and key stores to reduce exposure to credential harvesting or unauthorized extraction. Network and infrastructure systems (e.g., routing configurations, VPN policies, DNS/DHCP databases, IPAM records, PXE repositories, firmware images, and configuration templates) shall enforce strict write protections to prevent unauthorized modification that could lead to service disruption, spoofing, or persistent compromise. Security monitoring and response platforms shall enforce strict permissions on rule packs, dashboards, vulnerability reports, threat intelligence datasets, and forensic artifacts to prevent falsification, deletion, or suppression of evidence. At this level, file permissions reduce risk of unauthorized tampering, stored data manipulation, configuration abuse, credential exposure, and evidence deletion across mission and launch environments.	File permission enforcement shall evolve into dynamic, attribute-aware, and mission-context-driven access control across all endpoints and authoritative data stores. Attribute-Based Access Control (ABAC) shall be implemented where feasible, incorporating user role, device posture, mission phase, system criticality, and operational state into permission decisions. Write access to mission-critical artifacts (e.g., launch sequencing logic, abort criteria, command databases, cryptographic material, telemetry baselines, firmware repositories, monitoring rule sets, scheduling systems, and network configuration files) shall require just-in-time privilege elevation with automatic expiration and full audit traceability. Privileged write access shall not persist beyond defined operational tasks. Dual-authorization workflows shall be required for modification of safety-critical OT parameters, cryptographic key stores, scheduling priority rules, defensive configuration bundles, monitoring rule packs, and high-impact mission databases. No single account shall be capable of modifying authoritative artifacts and suppressing evidence of that modification. File permissions shall be continuously monitored for anomalous behavior, including unusual bulk reads, privilege escalation attempts, unexpected permission changes, or cross-role access patterns. Permission telemetry shall feed directly into SOC pipelines for correlation with authentication, logging, and operational state data. Strict controls shall prevent modification of boot artifacts, PXE repositories, firmware images, container images, update packages, DNS zone files, DHCP scopes, routing policies, VPN definitions, SIEM parsers, detection rules, SOAR playbooks, and forensic evidence stores. Unauthorized permission changes shall generate real-time alerts and may trigger automated containment actions. Adversary emulation shall validate that attempts to abuse valid accounts, escalate privileges, modify stored mission data, alter defensive logic, or tamper with key material are blocked or detected under both routine and mission-critical conditions. At this level, file permissions function as a mission integrity containment control, ensuring that authoritative mission data, cryptographic assets, scheduling logic, launch systems, monitoring platforms, and infrastructure configurations cannot be silently modified, deleted, or falsified even in the presence of compromised credentials or insider misuse.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-16	In limited areas where remote connectivity is mission-essential for operational continuity, maintenance, anomaly response, or vendor support, remote access shall be tightly controlled, explicitly authorized, and not continuously available by default. Remote connectivity shall be enabled only when operationally required and disabled when not actively in use. All remote access shall traverse dedicated VPN gateways or hardened jump hosts that enforce strong authentication and encrypted communications. Multi-factor authentication (MFA) shall be required for all remote operator, administrator, engineering, and vendor sessions. Remote access to controller interfaces, tracking systems, RF management systems, mission servers, planning workstations, telemetry processors, network devices, monitoring platforms, and cryptographic systems shall be limited to explicitly authorized roles. Vendor or contractor remote sessions shall be restricted to predefined time windows and require documented approval prior to connection. All remote sessions shall be logged, including authentication events, commands executed, configuration changes, and file access activity. Session activity shall be monitored and forwarded to centralized logging and security monitoring systems to enable investigation of credential misuse, remote service exploitation, or command abuse. Where feasible, remote commanding capabilities, particularly for launch systems and safety-critical OT controllers, shall be disabled entirely or restricted to read-only monitoring modes outside of approved operational windows. Remote access to launch control processors, sequencing systems, or abort logic components shall be tightly constrained and formally reviewed prior to mission-critical operations. Controlled remote access shall also apply to management-plane systems, including routers, firewalls, DNS/DHCP services, storage appliances, monitoring stacks, CI/CD runners, and IR tooling, as these systems represent high-value pivot points. At this level, remote access controls reduce exposure to exploitation of remote services, credential abuse, session hijacking, and unauthorized command execution across mission and launch environments.	In strictly defined and mission-essential scenarios, remote access shall operate under a default-deny posture and be dynamically enabled only when required for approved operational purposes. Persistent or always-on remote connectivity to mission, launch, OT, cryptographic, or management-plane systems shall be prohibited unless formally justified and risk accepted. When enabled, remote access shall operate under Zero Trust enforcement principles incorporating continuous authentication, device posture validation, certificate-based identity, and contextual risk evaluation prior to and throughout session establishment. All remote administrative sessions shall require certificate-based or hardware-backed authentication in addition to MFA. Device posture checks shall validate endpoint compliance prior to granting access to mission systems, launch infrastructure, network enforcement devices, or cryptographic services. Remote access to safety-critical systems (e.g., fueling controllers, launch sequencing logic, abort systems, antenna control units, RF switching infrastructure, and cryptographic management appliances) shall require dual-approval workflows during mission-critical phases such as launch campaigns. In many cases, remote commanding capability shall be fully disabled during high-impact operational windows unless explicitly authorized. Network micro-segmentation shall ensure that remote sessions are confined strictly to authorized systems and cannot pivot laterally into OT networks, cryptographic enclaves, telemetry databases, or monitoring infrastructure. Remote sessions to management planes, storage services, DNS/IPAM systems, SIEM platforms, DCO tooling, IR environments, and deception infrastructure shall be isolated from operational command paths. All remote sessions shall be recorded where operationally feasible, with full command capture and behavioral telemetry streamed into SOC pipelines for real-time correlation. Automated alerting shall detect abnormal session behavior such as off-hours access, rapid privilege escalation, unusual command sequences, unauthorized file access, or attempts to modify safety-critical parameters. Adversary emulation exercises shall validate that remote access mechanisms cannot be abused to pivot into fueling systems, manipulate telemetry processing, alter launch sequencing logic, tamper with monitoring platforms, or extract cryptographic material. Testing shall specifically validate resilience against exploitation of remote services, misuse of embedded remote access tools, VPN credential compromise, and session replay. At this level, remote access functions as a tightly constrained, continuously validated connectivity control that prevents unauthorized remote exploitation, restricts lateral movement, protects management planes, and preserves mission safety during both routine operations and high-impact launch phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-17	Service configurations across mission IT, ground control, telemetry processing, scheduling, monitoring, and supporting infrastructure systems shall be configured to operate with the minimum privileges necessary to perform their intended function. Services shall not run as root, Domain Administrator, or other highly privileged accounts unless explicitly required and formally justified. On Windows platforms, Managed Service Accounts (MSA/gMSA) shall be used where feasible to prevent credential reuse and reduce exposure to credential theft or abuse. Default service accounts, unused daemons, legacy protocols, and unnecessary background services shall be removed or disabled. Command and control services, scheduling engines, display/web services, monitoring collectors, DNS/DHCP services, NTP/PTP services, and other mission-support processes shall be configured to restrict privilege scope, limit system calls where supported, and prevent unauthorized modification or service stop actions. Service restart permissions and configuration modification rights shall be restricted to authorized administrators. Service configurations shall be reviewed at least quarterly and prior to mission-critical operations such as launch campaigns to ensure excessive privilege, misconfiguration, or unnecessary services have not been introduced. At this level, service configuration reduces privilege escalation pathways, limits abuse of service accounts, and prevents trivial disabling or manipulation of mission-critical services.	Service configurations shall be cryptographically protected, centrally enforced, and continuously validated against approved baselines using automated configuration management mechanisms. Service identities shall be tightly scoped, non-interactive, and protected with hardware-backed or vault-managed credentials where feasible. Integrity protection shall prevent unauthorized modification of service binaries, startup parameters, environment variables, authentication mechanisms, and restart policies. Continuous runtime monitoring shall validate that services operate under approved privilege levels and that unauthorized service activation, parameter modification, or privilege elevation attempts are immediately detected. Automated rollback or containment actions shall be triggered upon detection of unauthorized configuration changes, including restoration of approved configurations or isolation of affected endpoints. Mission-critical services (e.g., launch operations, telemetry ingestion, scheduling logic, time synchronization, security monitoring, identity infrastructure, and defensive tooling) shall undergo readiness validation prior to high-impact operational phases. Systems exhibiting unexplained privilege elevation, modified startup behavior, altered service dependencies, or weakened security parameters shall not proceed into operational states without formal review. Adversary emulation shall validate that misconfigured services cannot be leveraged for privilege escalation, service stop conditions, credential abuse, or defense impairment. At this level, service configuration operates as a continuous integrity and privilege enforcement mechanism that prevents service-level misconfiguration from becoming a pivot point for compromise of mission, launch, or ground control systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-18	Least-privilege access shall be enforced across all ground users, operators, engineers, administrators, analysts, and automated service accounts. Role-Based Access Control (RBAC) shall ensure that users are granted only the minimum permissions required to perform their assigned duties within mission operations, launch activities, monitoring environments, scheduling systems, configuration management platforms, and supporting infrastructure. Access to sensitive functions such as command submission, configuration modification, firmware updates, cryptographic material handling, routing changes, or schedule overrides shall be restricted to explicitly authorized roles. Privileges shall be formally provisioned through documented workflows and reviewed periodically to identify excessive or unused entitlements. Unused accounts, shared credentials, and legacy privilege assignments shall be removed. Write, delete, and approval permissions for authoritative mission artifacts, monitoring configurations, and operational data stores shall be limited to designated roles to prevent unauthorized modification or destruction. Personnel shall receive training reinforcing why privilege restrictions are necessary to protect mission integrity and reduce the impact of credential compromise. At this level, least-privilege enforcement reduces the blast radius of compromised credentials, limits misuse of valid accounts, and prevents a single stolen identity from exercising broad operational or administrative control.	Least-privilege enforcement shall be elevated to dynamic, policy-driven privilege management integrated with Privileged Identity Management (PIM) or Privileged Access Management (PAM) platforms. Privileged access shall be provisioned using JIT elevation mechanisms with automatic expiration upon completion of authorized tasks. Privilege escalation during mission-critical windows, including launch campaigns, command loads, fueling operations, or high-risk operational phases, shall require dual approval and formal authorization. All elevated sessions shall be logged, recorded where feasible, and streamed to SOC monitoring pipelines for anomaly detection and correlation with authentication, endpoint, and operational telemetry. Automated controls shall detect privilege creep, unusual combinations of access, cross-role activity, or anomalous use of elevated permissions. Privilege assignments affecting high-value systems, cryptographic material, scheduling overrides, detection infrastructure, or safety-critical configurations shall be continuously monitored for misuse or abnormal behavior. Adversary emulation shall validate that attempts to abuse valid credentials, escalate privileges, or leverage compromised accounts to gain broader authority are detected and contained. At this level, user least privilege functions as a structural containment control that prevents valid-account abuse from escalating into mission-wide compromise and ensures that no single compromised identity can independently manipulate high-impact mission systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
END-19	Authenticated vulnerability scanning shall be performed at least monthly across all ground IT endpoints, including mission servers, C2 systems, telemetry processors, dashboards, orchestration portals, storage systems, scheduling platforms, security monitoring infrastructure, and network devices. Scanning shall identify operating system vulnerabilities, exposed services, misconfigurations, weak authentication paths, and outdated COTS components that could be exploited through remote service abuse or public-facing application exploitation. Public-facing interfaces such as dashboards, telemetry APIs, scheduler portals, federation gateways, and orchestration services shall receive prioritized scanning coverage due to elevated exposure risk. Security infrastructure platforms including SIEM, EDR, IDS, SOAR, monitoring collectors, and IR toolchains shall also be included in scope to reduce the likelihood of defense tool exploitation. For OT and ICS environments, vulnerability assessments shall be conducted in controlled test environments or offline laboratories to prevent operational disruption. When direct scanning of production OT systems is not feasible, validated compensating techniques such as configuration review, vendor advisories, and firmware analysis shall be used. Scan results shall feed directly into patch management workflows with tracked remediation timelines and documented risk acceptance where applicable. Coverage maps shall be maintained to clearly identify which assets are scanned, when they were last assessed, and which systems lack vulnerability visibility. Mission management shall receive periodic risk posture summaries reflecting vulnerability trends and remediation status. At this level, vulnerability scanning provides structured visibility into exploitable weaknesses and reduces exposure to remote exploitation, service abuse, and defense tool compromise across mission environments.	Vulnerability scanning shall evolve into a continuous, authenticated assessment capability integrated with SIEM dashboards and risk tracking systems. Critical IT assets shall be scanned on a near-continuous or weekly cadence, with automated ingestion of findings into centralized risk registers and mission assurance reporting processes. Strict remediation timelines shall be enforced based on severity and mission impact, with compliance tied to mission readiness gates. Critical vulnerabilities affecting mission management systems, C2 platforms, public-facing services, network enforcement devices, monitoring infrastructure, cryptographic systems, or launch-support endpoints shall be remediated within defined maximum windows or formally waived at leadership level prior to operational progression. For OT environments, maintained digital twins or parallel testbeds shall be used to safely validate vulnerabilities, patches, and exploit conditions prior to production changes. Vulnerability discovery affecting firmware, control logic, time services, scheduling APIs, storage systems, and security appliances shall trigger structured impact analysis aligned to mission phase. Independent third-party vulnerability assessments shall be conducted annually to provide objective validation of internal scanning coverage, methodology, and blind spots. Scan telemetry and remediation status shall be continuously visible within SOC dashboards to enable correlation with authentication events, endpoint alerts, file integrity findings, and operational anomalies. Adversary emulation shall validate that exploitable conditions identified through scanning cannot be leveraged during high-impact mission windows, including launch campaigns or critical operational phases. At this level, vulnerability scanning functions as a continuous exposure management capability that proactively identifies, prioritizes, and drives remediation of weaknesses before they can be operationalized by adversaries against mission-critical systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-1	Reverse proxies shall be deployed in front of all mission-facing web applications and API endpoints, including dashboards, telemetry viewers, sequencing tools, approval portals, scheduling interfaces, visualization services, management consoles, and externally accessible orchestration platforms. Public-facing services shall not expose backend systems directly. Reverse proxies shall enforce TLS 1.2 or higher using modern cipher suites and HSTS to prevent downgrade attacks and plaintext access. All access shall integrate with centralized identity systems, requiring Single Sign-On (SSO) and multi-factor authentication for authenticated services. Rate limiting, request size limits, per-route restrictions, and input validation shall be enabled to minimize exposure of unnecessary functionality. Reverse proxies shall be deployed within a properly segmented DMZ separate from mission IT and OT networks to prevent direct pivoting into telemetry processors, C2 systems, launch infrastructure, or control networks. Logging shall capture request metadata sufficient to detect anomalous patterns or attempted exploitation. Penetration testing shall be conducted prior to mission-critical campaigns to validate that public-facing interfaces cannot be trivially exploited through injection, misrouting, or authentication bypass conditions. At this level, reverse proxies reduce exposure to Exploit Public-Facing Application (T1190), command-and-control over web protocols (T1071), service abuse, and opportunistic injection attacks by enforcing a hardened boundary between external users and mission systems.	Reverse proxies shall function as hardened trust boundaries for all mission web services and APIs. TLS 1.3 shall be required, with mutual TLS (mTLS) enforced between proxy layers and backend services to prevent backend impersonation or lateral abuse. Cipher suites shall be strictly allowlisted, certificates shall be validated against pinned trust anchors where feasible, and session tokens shall be short-lived and cryptographically bound to user and device context. Fine-grained access control shall be enforced through integration with ABAC or policy engines, enabling dynamic restriction of telemetry views, command interfaces, approval actions, and scheduling capabilities based on role, mission phase, device posture, and risk indicators. Proxies shall enforce deep request validation, anomaly detection, and adaptive rate controls to mitigate injection attempts, authentication bypass, API abuse, defacement, and denial-of-service conditions. All proxy logs shall be cryptographically protected and streamed in real time to SOC monitoring pipelines with integrity validation to prevent tampering. Reverse proxy resilience shall be validated through red-team adversary emulation prior to mission-critical campaigns, specifically testing injection attacks, routing manipulation, header spoofing, authentication bypass, rate-limit evasion, and backend pivot attempts. At this level, reverse proxies serve as cryptographically enforced, policy-driven security gateways that prevent direct exploitation of mission web services, constrain attack surface, and provide high-assurance inspection and enforcement during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-2	Access Control Lists (ACLs) shall enforce a default-deny posture at all logical network boundaries within the ground architecture, including between enterprise IT, mission IT, OT networks, launch environments, partner enclaves, and externally facing services. Only explicitly authorized protocols, ports, hosts, and services required for mission operations (e.g., telemetry transport, command pathways, approved ICS protocols such as Modbus/TCP where applicable) shall be permitted. ACLs shall explicitly restrict which systems may communicate with antenna control units, tracking servers, calibration services, RF switching systems, SDR controllers, sequencing services, launch control processors, scheduling APIs, storage platforms, time servers, authentication endpoints, and other mission-critical services. Unauthorized lateral communication attempts shall be blocked and logged. ACL configurations shall be documented, version controlled, and reviewed at least quarterly and prior to mission-critical operations such as launch campaigns. ACL hit and deny events shall be forwarded to centralized logging or SIEM platforms for monitoring. Operators shall be trained to interpret unexpected deny events as potential reconnaissance, probing, or exploitation attempts rather than routine noise. ACL rules shall be validated during rehearsals and pre-mission testing to ensure mission-critical traffic is not inadvertently blocked while maintaining strict least-privilege network segmentation. At this level, ACLs reduce exposure to Exploitation of Remote Services (T1210), Exploit Public-Facing Applications (T1190), lateral movement, unauthorized ICS communication (e.g., T0814, T0855), and data manipulation paths (T1565) by enforcing deterministic communication boundaries between mission systems.	ACL enforcement shall be cryptographically controlled, continuously validated, and tightly integrated with mission assurance workflows. ACL configurations shall require cryptographic integrity protection and attestation prior to deployment, ensuring that routing and enforcement policies cannot be silently altered. Continuous compliance scanning shall validate deployed ACLs against approved baseline configurations. Deviations shall trigger alerts and require formal review. During mission-critical windows such as launch campaigns, ACL modifications shall require dual approval and shall be time-bound where feasible. ACL telemetry shall be integrated with authentication logs, anomaly detection systems, and physical telemetry feeds. For example, denied traffic targeting fueling PLCs, launch control processors, or cryptographic endpoints during countdown shall generate elevated mission alerts and may trigger automated no-go or containment workflows. Immutable logging shall be enforced for ACL change history, hit/deny events, and management-plane access to network enforcement devices. Logs shall be stored in tamper-resistant storage suitable for forensic reconstruction following launch or operational events. Adversary emulation shall validate that ACL segmentation prevents unauthorized communication to ICS/OT systems, command pathways, scheduling databases, crypto control planes, storage systems, and identity providers. Testing shall confirm that stealthy adversary attempts to pivot, bypass segmentation, manipulate routing paths, or stage MITM positioning (T1557) are detected and contained. At this level, ACLs function as high-assurance network containment controls that cryptographically protect segmentation boundaries, constrain lateral movement, prevent unauthorized control-plane access, and provide forensic-grade visibility during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-3	Multi-factor authentication (MFA) shall be required for all IT operator and administrative accounts that manage network infrastructure, including routers, switches, firewalls, VPN concentrators, console servers, DNS/DHCP/IPAM platforms, crypto appliances, and federation gateways. Legacy management protocols and unsecured authentication mechanisms shall be disabled. Shared vendor or default administrative accounts on network and OT-connected devices shall be replaced with named accounts tied to individual identities. Where native MFA is not supported on infrastructure devices, administrative access shall be restricted through hardened jump hosts that enforce MFA prior to session establishment. Device authorization controls shall ensure that only approved administrative workstations may connect to network enforcement devices or management planes. Unmanaged or rogue endpoints shall be prevented from accessing management interfaces. Separate identities shall be maintained for IT network administration and OT/mission network operations to prevent convergence of privileges across environments. Administrative access paths shall be documented and reviewed at least quarterly and prior to mission-critical events such as launch campaigns. Dormant, orphaned, or terminated accounts shall be removed immediately. At this level, strong authentication reduces the likelihood of credential-based takeover of routing infrastructure, VPN gateways, DNS/DHCP services, console servers, and crypto devices, mitigating Valid Account abuse (T1078), authentication modification attempts (T1556), and remote service exploitation (T1210).	Network administration shall align with Zero Trust identity enforcement principles across IT and OT infrastructure. Authentication decisions shall incorporate continuous validation of user identity, device posture, network location, and mission phase before granting or maintaining privileged access to network enforcement devices. Certificate-based or hardware-token-backed authentication shall be required for all privileged access to routers, switches, firewalls, VPN concentrators, DNS/DHCP/IPAM systems, console servers, crypto appliances, and identity components. Administrative access shall originate only from hardened privileged access workstations (PAWs) or equivalent secured management environments. Just-in-time privileged access shall be enforced for network administration roles, with automatic expiration of elevated privileges. Dual-approval workflows shall be required for high-impact changes during mission-critical windows, including modifications to routing policies, ACLs, crypto enforcement settings, VPN configurations, trust relationships, or DNS zone configurations. Authentication telemetry from all network management planes shall stream into SOC monitoring systems for correlation with ACL changes, configuration drift, file integrity alerts, and physical telemetry events. Automated analytics shall detect anomalous administrative behavior such as off-hours access, rapid configuration changes, geographically inconsistent logins, or privilege escalation attempts. Adversary emulation shall validate that attempts to abuse valid credentials, replay tokens, compromise VPN gateways, or reconfigure crypto enforcement (e.g., T1078, T1556, T1550) are detected and either blocked or escalated immediately. At this level, network administrative authentication functions as a continuously validated identity assurance boundary protecting management planes, routing control, cryptographic enforcement points, and trust infrastructure from credential-only compromise and privilege abuse during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-4	Golden configuration baselines shall be established and maintained for each network device role, including routers, switches, firewalls, VPN concentrators, DNS/DHCP/IPAM platforms, console servers, crypto appliances, monitoring taps, and partner connectivity gateways. Approved configurations shall be stored in version-controlled repositories and tied to formal change management tickets to ensure traceability and accountability. Network provisioning and configuration updates shall be automated where feasible using infrastructure-as-code mechanisms (e.g., Ansible or equivalent tooling) to reduce manual drift and ensure consistent deployment across enclaves, including launch control networks and mission operations environments. All configuration changes shall require documented review and approval prior to deployment. Monthly compliance scans shall validate adherence to secure configuration standards, including enforcement of SNMPv3-only management, SSHv2-only remote access, centralized syslog logging, authenticated time synchronization, and removal of default credentials. Insecure or legacy protocols and daemons shall be disabled by policy and verified through automated checks. Running and startup configurations shall be backed up regularly and stored securely to enable rapid restoration in the event of misconfiguration, corruption, or unauthorized modification. Configuration backups shall be protected from tampering and access-controlled. At this level, structured network configuration management reduces the likelihood of unauthorized or unsafe changes to routing, firewall rules, VPN policies, trust relationships, and protocol parameters that could enable exploitation of remote services (T1210), silent traffic manipulation (T1565.003), or service disruption (T1489).	Network configurations shall be cryptographically signed and validated prior to load or activation on production devices. Configuration files shall require integrity verification checks during deployment, and unauthorized or unsigned configurations shall be rejected automatically. All network configuration changes shall be managed through CI/CD-style deployment pipelines with peer review, cryptographic approval, and automated validation prior to production promotion. Configuration repositories shall be tamper-evident and enforce strict access controls to prevent unauthorized modification of routing tables, firewall rules, VPN policies, crypto settings, DNS/DHCP configurations, and federation trust parameters. Automated rollback mechanisms shall be implemented to restore devices to last known-good states when unauthorized or insecure configuration changes are detected. Real-time drift detection shall continuously compare live device states against approved baselines, triggering alerts and containment actions when deviations occur. Cryptographic attestation of device configurations shall occur at boot and periodically during runtime to validate that enforcement policies, ACLs, routing parameters, logging settings, and management-plane controls remain intact. Configuration change events shall stream directly into SOC pipelines for correlation with authentication logs, ACL denials, file integrity alerts, and physical telemetry. Insecure protocols shall be disabled by enforced policy (e.g., mandatory SNMPv3, SSHv2, strong cipher suites), and compliance violations shall block progression into mission-critical phases such as launch campaigns unless formally reviewed and approved. Adversary emulation shall validate that attempts to silently alter routing paths, weaken authentication settings, modify VPN trust relationships, disable logging, or reroute monitored traffic (e.g., T1556, T1565.003, T1199) are detected and either prevented or immediately escalated. At this level, network configuration management functions as a cryptographically enforced integrity control that prevents silent manipulation of routing, firewall, VPN, and trust infrastructure and ensures tamper-evident, rapidly recoverable network posture during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-5	Network devices supporting mission operations, launch infrastructure, and OT control networks shall be hardened using industry-recognized benchmarks such as CIS or DISA STIG guidance. Unnecessary services including Telnet, HTTP (unencrypted), Cisco Smart Install, legacy SNMP versions, and unused management daemons shall be disabled. Only secure management protocols such as SSHv2 and HTTPS with modern cipher suites shall be permitted. SNMPv3 with authentication and encryption shall be required for network monitoring and management functions. Default accounts, shared credentials, and vendor-provided credentials shall be removed or disabled, and unique named administrative accounts shall be enforced where supported. Physical and logical access to management interfaces, console ports, out-of-band (OOB) management paths, and uplink interfaces shall be restricted to authorized personnel and controlled network segments. Access to routing engines, firewall management planes, VPN concentrators, and protocol control planes shall be limited to hardened administrative workstations. Cryptographic configurations shall be reviewed to ensure that only modern algorithms (e.g., stronger hashing, secure IKE/IPsec modes, strong TLS cipher suites) are permitted. Weak or deprecated algorithms, insecure protocol fallbacks, and legacy key exchange mechanisms shall be disabled. Network-layer protections such as DHCP snooping, dynamic ARP inspection, and rate limiting shall be enabled where feasible to reduce exposure to denial and man-in-the-middle staging attempts. At this level, network device hardening reduces exploitability of switches, routers, firewalls, and VPN appliances that adversaries frequently target to gain control of traffic paths, pivot into OT enclaves, or manipulate command and telemetry routing (e.g., T1190, T1210, T1557).	Network devices shall implement secure boot with hardware-backed attestation to validate firmware and operating system integrity at startup. Only cryptographically signed firmware images from trusted sources shall be permitted to load, and firmware integrity shall be periodically verified during runtime where supported. All cryptographic functions on network devices shall use FIPS-validated modules, and devices shall enforce strong cipher allowlists with downgrade protection mechanisms to prevent fallback to insecure modes. Weak IKE configurations, legacy TLS versions, insecure management protocols, and unused crypto services shall be cryptographically disabled rather than merely administratively turned off. Continuous posture monitoring shall validate that unused ports remain disabled, insecure services are not re-enabled, and management planes remain restricted to approved administrative enclaves. Automated remediation mechanisms shall disable newly enabled insecure services or revert unauthorized configuration changes to last known-good states. Management-plane hardening status, firmware integrity validation events, and service activation changes shall stream into SOC pipelines for correlation with authentication logs, ACL events, and anomaly detection systems. Real-time alerts shall trigger when routing control planes, VPN termination points, or firewall enforcement mechanisms deviate from approved security posture. Configuration exceptions during mission-critical phases such as launch campaigns shall require multi-person approval workflows. Third-party validation or independent integrity checks shall be required for firmware updates or major configuration changes affecting routing, VPN trust relationships, or OT enclave boundaries. Adversary emulation shall validate that exploitation attempts against management interfaces, protocol handlers, or crypto enforcement points are either prevented or immediately detected, particularly those that would enable pivoting into control networks or manipulation of mission traffic paths (e.g., T1210, T1557, T1600.002). At this level, network device hardening functions as a control-plane integrity enforcement mechanism, preventing silent manipulation of routing, crypto enforcement, and traffic-handling logic that could otherwise enable mission-impacting compromise during high-impact operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-6	Where mission-essential and operationally feasible, redundant network paths shall be provisioned between mission enclaves, ground stations, launch infrastructure, and supporting enterprise services to reduce single points of failure. Redundant switches, routers, uplinks, and physical cabling shall be implemented for mission-critical systems including command uplink paths, telemetry ingest pipelines, dashboards, and OT controller communications. Control plane (command) traffic and data plane (telemetry, science, and monitoring data) traffic shall be logically or physically separated where feasible to reduce the risk that congestion, failure, or attack on one plane disrupts the other. Network architecture documentation shall explicitly identify single points of failure and existing failover mechanisms. Failover mechanisms shall be periodically tested to validate continuity of operations under degraded conditions. Operators shall be trained on manual failover procedures where automated failover is not available. Redundancy and path resiliency shall be incorporated into mission resilience planning and rehearsals, including launch readiness reviews. At this level, path redundancy and separation reduce the operational impact of flooding or destabilization attempts against mission uplink, downlink, gateway, or transport paths, improving resilience against denial-of-service style disruptions (e.g., T1498).	Mission-critical network flows, including command uplink, telemetry ingest, launch control data, gateway services, and OT management traffic, shall be architected with physically and geographically diverse paths. Redundant circuits shall not share common physical conduits, power domains, or upstream providers where feasible, reducing susceptibility to coordinated disruption. Active/active or hot-standby routing configurations shall be implemented with automatic failover and rapid convergence to minimize interruption of mission services. Sub-second convergence mechanisms shall be configured where supported for command and launch-critical paths. Separation of control and data planes shall be enforced with independent routing policies and monitoring. Continuous monitoring shall assess path health, latency anomalies, routing instability, and unexpected path changes. Alerts indicating route manipulation or degradation shall be integrated into NOC and SOC workflows for immediate triage. Failover capabilities shall be exercised under live or realistic mission loads, including rehearsal scenarios simulating flooding, link loss, gateway disruption, or transport instability. Results shall be documented and incorporated into mission assurance reviews. Network path diversity and resilience shall be incorporated into mission certification criteria and validated through resilience exercises and adversary emulation scenarios targeting denial-of-service, routing manipulation, or gateway destabilization (e.g., T1498). At this level, network path diversification functions as a mission continuity assurance mechanism, ensuring that adversarial disruption of a single transport path cannot interrupt command, telemetry, or launch-critical operations during high-impact mission phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-7	Current Layer 2 and Layer 3 network diagrams shall be maintained to clearly depict separation between IT and OT environments, including VLAN segmentation, ACL boundaries, firewall zones, DMZs, routing domains, and defined trust boundaries. Diagrams shall explicitly document mission-critical flows, including command uplink paths, telemetry ingest pipelines, external data distribution channels, launch data interfaces, and inter-enclave communications. Port and protocol matrices for command and telemetry (CMD/TLM) paths shall be documented and validated to ensure only required services are exposed. Network diagrams shall be updated prior to each major mission milestone, including significant architecture changes, partner integrations/interconnections, and launch campaigns. Diagrams shall be stored in a shared, access-controlled repository to ensure availability to authorized engineering, cybersecurity, and operations personnel. Documentation shall be reviewed during security assessments, quarterly governance reviews, and after significant network modifications. Network diagrams shall be used during incident response activities to rapidly identify trust zones, containment boundaries, choke points, and affected data paths. At this level, accurate and current documentation provides authoritative visibility into trust relationships and segmentation controls, enabling defenders to execute containment, validate ACL enforcement, and assess potential manipulation or man-in-the-middle paths (e.g., T1557, T1565.003) during active incidents.	Network documentation shall be version-controlled, digitally signed, and integrated into formal change management workflows to ensure authoritative and tamper-evident architectural records. All updates to network segmentation, ACL policies, firewall zones, routing policies, or trust boundaries shall require corresponding diagram updates prior to change approval. Network diagrams shall be integrated with CM database and asset inventory systems and continuously validated against actual device configurations using automated discovery and modeling tools. Where feasible, operational network modeling platforms (e.g., RedSeal, Forward Networks, or equivalent) shall be used to generate topology views directly from device configurations, ensuring real-time architectural fidelity. Diagram outputs shall directly inform threat modeling activities, red and blue team exercises, detection engineering, and segmentation validation efforts. Trust boundaries, choke points, and monitoring coverage areas shall be explicitly mapped to defensive controls and telemetry sources to ensure no blind spots exist in monitoring or enforcement. Continuous automated discovery tools (e.g., RedSeal, Forward Networks, or equivalent) shall reconcile live device states against documented architectures, generating alerts when unauthorized topology changes, route modifications, or segmentation drift occur. Diagram fidelity shall be validated during mission readiness reviews and resilience exercises. At this level, network documentation functions as a continuously validated architectural integrity control, ensuring that segmentation assumptions, trust boundaries, and data paths remain accurate, enforceable, and defensible during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-8	Internal firewalls shall be deployed between mission enclaves to enforce explicit trust boundaries and least-privilege connectivity using a default-deny model. Only explicitly authorized command, telemetry, planning, scheduling, analytics, and management flows shall be permitted between zones. For example, uplink servers may communicate with ground station interfaces, telemetry ingest systems may forward data to processing tiers, and operator consoles may query telemetry databases, but direct access to uplink servers, launch control systems, PLC interfaces, or key management infrastructure shall be restricted unless explicitly required. Firewalls shall enforce segmentation between enterprise IT, mission operations networks, OT/ICS environments, launch control enclaves, analytics tiers, and monitoring systems to reduce lateral movement risk following compromise. Zone boundaries shall be documented and validated against mission architecture diagrams. All allowed and denied traffic shall be logged and forwarded to centralized monitoring systems. Firewall rule sets shall be reviewed quarterly and prior to mission-critical phases such as launch campaigns to ensure temporary allowances have not expanded beyond operational necessity. At this level, internal firewalls constrain lateral pivoting (e.g., T1210), reduce exposure to exploitation of remote services (T1190), and limit blast radius if a single enclave is compromised.	Internal firewalls shall enforce Zero Trust micro-segmentation across all mission enclaves, including separation of command processing, telemetry ingestion, analytics tiers, operator networks, OT/ICS control systems, cryptographic infrastructure, monitoring platforms, and partner ingress points. Policies shall implement default-deny zoning with tightly scoped allowlists aligned to mission data flows and operational roles. Next-generation firewalls shall be used where appropriate to provide deep packet inspection and protocol validation for mission-specific traffic (e.g., CCSDS TM/TC/AOS/SLE and other ground-specific protocols), preventing malformed, unauthorized, or unexpected control sequences from traversing enclave boundaries. Firewall configurations shall be continuously validated against cryptographically protected golden baselines using automated policy compliance checks. Firewall telemetry shall stream into SOC pipelines for correlation with endpoint authentication events, file integrity alerts, application logs, and OT telemetry. Correlation rules shall detect attempts to pivot between telemetry, launch, planning, scheduling, or cryptographic environments following credential compromise or exploitation. During mission-critical windows, firewall rule changes shall require dual authorization and generate heightened monitoring. Red-team adversary emulation shall validate that firewall boundaries prevent lateral movement between enterprise IT and launch control networks, between analytics tiers and command systems, and between partner ingress points and mission enclaves. At this level, internal firewalls function as hardened, continuously validated containment controls that enforce architectural trust boundaries, prevent cross-enclave pivoting, and preserve mission integrity during high-impact operational phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-9	Detailed logging shall be enabled on all routers, switches, firewalls, VPN concentrators, crypto gateways, and other network infrastructure supporting mission operations. Logging shall capture ACL hits and denials, control-plane events, routing changes, failed authentication attempts, configuration modifications, VPN session activity, crypto negotiation failures, and abnormal protocol usage. Logs shall be forwarded to a centralized SIEM or SOC monitoring platform to prevent local tampering and to enable correlation with endpoint, application, and mission telemetry events. Retention periods shall align with mission policy, with a minimum of 180 days or longer where required for mission lifecycle or regulatory requirements. Network logging shall provide visibility into anomalous command paths, unexpected data flows, MITM attempts, remote service exploitation attempts, brute-force authentication activity, DoS precursors, abnormal DNS/DHCP behavior, suspicious VPN usage, and unexpected telemetry or API access patterns. Logs shall be reviewed at least weekly as part of routine security operations, with heightened review prior to and during mission-critical phases such as launch campaigns. At this level, network logging provides foundational visibility into traffic manipulation, ACL abuse, routing anomalies, authentication failures, and protocol misuse, supporting detection of exploitation, denial-of-service, and lateral movement attempts (e.g., T1557, T1210, T1498, T1565).	Network logging shall be real-time, tamper-evident, and tightly integrated into SOC detection workflows. All network devices shall generate cryptographically protected logs, with integrity validation mechanisms ensuring that configuration changes, ACL modifications, routing updates, crypto failures, and authentication events cannot be altered or suppressed without detection. Logs shall stream continuously into SIEM/SOC platforms for automated correlation with endpoint telemetry, identity events, OT control data, and mission telemetry anomalies. Anomaly detection shall identify suspicious patterns such as abnormal ACL denials toward fueling controllers or uplink systems, unexpected routing changes affecting command paths, anomalous VPN access during restricted mission phases, replay behavior, traffic redirection attempts, or crypto downgrade events. Long-term log retention shall align with the full mission lifecycle to support forensic reconstruction, regulatory compliance, and post-incident mission assurance review. Immutable storage mechanisms shall be used to preserve high-value network logs. Automated alerting shall trigger on high-risk events such as unauthorized configuration changes during launch windows, unexpected control-plane modifications, or anomalous flows between enterprise IT and mission enclaves. During mission-critical operations, configuration changes and associated log events shall require dual authorization and heightened monitoring. Red-team adversary emulation shall validate that attempts to manipulate routing, bypass ACLs, stage MITM positioning, exploit VPN gateways, or suppress logging generate detectable and actionable alerts. At this level, network logging functions as a mission-integrity visibility layer, enabling rapid detection of traffic manipulation, denial-of-service staging, credential abuse, routing compromise, and cross-enclave pivot attempts during high-impact operational phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-10	Network Access Control (NAC) shall be deployed across all wired and wireless access points supporting mission networks to enforce device validation prior to granting network access. All consoles, engineering laptops, operator workstations, and administrative systems shall undergo posture validation before joining mission VLANs or management enclaves. Validation checks shall include patch status, anti-virus/EDR presence, configuration compliance, and domain enrollment where applicable. Unknown, unmanaged, or non-compliant devices shall be automatically placed into restricted VLANs or quarantine segments with no access to mission command, telemetry, launch, or OT control systems. NAC policies shall prevent rogue administrator laptops, unauthorized partner systems, or unmanaged devices from attaching to sensitive enclaves. For OT environments where full posture validation may not be technically feasible, MAC-based controls, certificate-based device identity, or equivalent mechanisms shall restrict network participation to known and authorized devices. NAC enforcement shall ensure that only approved devices may obtain DHCP leases, participate in DNS resolution, or access mission-critical VLANs. All NAC events, including authentication attempts, posture failures, and quarantine actions, shall be logged and forwarded to centralized SIEM/SOC platforms for monitoring. Security teams shall review unauthorized access attempts to identify probing, credential abuse, rogue device staging, or lateral movement preparation (e.g., T1078, T1210, T1040, T1557). At this level, NAC reduces risk from unmanaged devices, rogue admin systems, unauthorized partner endpoints, and device-based pivot attempts into mission or launch enclaves.	Network Access Control shall enforce cryptographically bound device identity with hardware-backed assurance. All mission-connected endpoints shall use certificate-based authentication, with device identity anchored to hardware roots of trust (e.g., TPM, HSM, or equivalent). Devices shall not be granted network access solely on user credentials. Continuous posture validation shall be enforced such that devices drifting out of compliance (e.g., missing patches, disabled EDR, altered baseline configurations) are automatically quarantined or restricted in real time. Enforcement shall apply across mission IT, engineering networks, management enclaves, and, where supported, OT networks. For OT controllers and embedded devices, boot-time attestation shall validate firmware integrity and configuration state prior to network admission. Devices failing integrity checks shall be denied connectivity to operational networks. Exceptions, including temporary vendor laptops or specialized equipment, shall require documented justification and dual-approval workflows, particularly during mission-critical phases such as launch campaigns or command load operations. NAC compliance shall be tied to mission readiness gates such that non-compliant devices can prevent progression into operational states. NAC telemetry shall stream continuously into SOC pipelines for automated correlation with authentication events, firewall denials, lateral movement attempts, DHCP anomalies, DNS abuse, and ARP poisoning indicators. Detection logic shall identify rogue device staging, unauthorized name-resolution participation, DHCP starvation attempts, and unmanaged endpoints attempting MITM positioning (e.g., T1040, T1557.002, T1498, T1499). Adversary emulation shall validate that rogue devices, unmanaged laptops, credential-only attacks, and posture-evasion attempts are detected, quarantined, and correlated with mission security telemetry. At this level, NAC functions as a Zero Trust device authorization control, ensuring that only cryptographically validated, posture-compliant, and hardware-bound devices can participate in mission networks, thereby significantly reducing rogue device risk and lateral pivot opportunities during high-impact mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-11	A dedicated Network Operations Center (NOC) capability shall monitor availability, throughput, latency, and alert conditions across IT and OT network segments supporting mission and launch operations. Monitoring shall include path health for telemetry ingest, command uplink paths, fueling infrastructure connectivity, antenna control networks, and critical data distribution flows. Dashboards shall provide real-time visibility into link status, bandwidth utilization, packet loss, and failover state across mission-critical paths. NOC personnel shall maintain situational awareness during routine operations and heightened vigilance during mission-critical phases such as launch campaigns, fueling operations, or active spacecraft commanding. Scheduled maintenance windows shall be formally coordinated to avoid disruption of mission readiness or launch timelines. Regular failover drills shall be conducted to validate redundancy between switches, routers, firewalls, uplink paths, and ground station interfaces. Documented procedures shall ensure that operators can transition between redundant paths without introducing unsafe states. NOC alerts shall be integrated with SOC monitoring systems to enable unified cyber and operational visibility. Correlation between availability degradation and security telemetry shall be reviewed to detect potential denial-of-service conditions, routing instability, or service disruption attempts (e.g., T1498, T1499, T1489). At this level, the NOC operationalizes availability monitoring and rapid response to outages, ensuring that flooding, blackholing, or routing disruptions cannot silently persist long enough to deny mission operations. The NOC monitors operational availability and network health, whereas the SOC monitors adversary activity and cybersecurity threats.	The NOC shall function as a mission-fused operational capability that correlates network telemetry with spacecraft, antenna, and OT system state in coordination with the SOC. Network availability, latency, jitter, routing changes, and packet loss shall be continuously correlated with mission events such as fueling operations, command uplinks, spacecraft maneuver windows, telemetry downlink passes, and launch countdown milestones. Automated anomaly detection shall identify latency spikes, jitter fluctuations, routing instability, or traffic shaping conditions that could degrade telemetry integrity or command reliability. Alerts shall be prioritized according to mission phase, with defined escalation paths tied to launch hold, abort, or no-go decision logic where network degradation presents safety or mission risk. NOC capabilities shall include geographically distributed staff and redundant operational facilities to ensure continuity during regional outages, natural disasters, or targeted infrastructure disruption. Operator actions within the NOC, including routing adjustments, failover activations, or policy overrides, shall be cryptographically logged and retained in tamper-evident storage for accountability and post-event forensic analysis. NOC telemetry shall stream in real time to SOC fusion dashboards, enabling correlation between network anomalies, authentication events, endpoint detections, and OT telemetry deviations. This integrated awareness shall detect coordinated attacks such as DDoS combined with credential misuse or routing manipulation designed to mask malicious activity (e.g., T1498, T1499, T1562). Adversary-in-the-loop red-team exercises shall simulate distributed denial-of-service, BGP/route manipulation, link flooding, or staged path degradation attacks during mission rehearsal scenarios to validate operator readiness, detection fidelity, and decision-making under time-constrained launch conditions. At this level, the NOC becomes a mission assurance control, ensuring that network availability, integrity, and performance are continuously validated against mission context and that operational decisions are informed by fused cyber and infrastructure telemetry during high-impact mission operations. The NOC owns mission availability and routing stability decisions, whereas the SOC owns adversary detection and containment; fusion occurs during mission-critical operations but operational authority remains clearly separated.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-12	Authenticated and hierarchically controlled NTP/PTP services shall be deployed using trusted GNSS-sourced master clocks. All mission-critical devices (e.g., mission servers, operator consoles, telemetry ingestion systems, C2 infrastructure, network devices, and OT controllers) shall synchronize to designated trusted time sources. A defined fallback hierarchy shall provide redundancy without allowing uncontrolled external time sources. Time synchronization shall be monitored continuously for drift, offset anomalies, and synchronization failures, with alert thresholds established to detect potential manipulation or degradation. Access Control Lists (ACLs) and firewall rules shall restrict which systems may provide or request time services to prevent rogue time injection. Time integrity shall be validated during mission-critical phases, including pre-launch rehearsals and launch operations, to ensure reliable command ordering, telemetry correlation, log reconstruction, and abort logic sequencing. At this level, network time services provide consistent and authenticated temporal reference necessary for forensic reconstruction, anomaly detection, and coordinated mission operations.	Network time distribution shall be cryptographically authenticated and integrity-protected using secure NTP/PTP configurations with hardware timestamping where required for microsecond-level precision. Time sources shall leverage physically diverse GNSS receivers and redundant time distribution paths to mitigate spoofing, jamming, or single-point failure scenarios. All time servers shall enforce strict stratum control (hierarchy), authenticated peers, and explicit allowlists of authorized clients. External or unauthorized NTP/PTP sources shall be blocked by policy at network boundaries. Time drift, synchronization failures, leap events, and offset anomalies shall stream in real time to SOC correlation pipelines, where deviations are analyzed as potential indicators of adversary manipulation, replay staging, log tampering, or coordinated control-plane attack activity. Time integrity validation shall be integrated into mission readiness gates, with explicit verification prior to launch, fueling, or critical command operations. Red-team and adversary emulation exercises shall include GPS spoofing, NTP manipulation, replay timing abuse, and selective time skew scenarios to validate resilience and detection capability. All logs, telemetry, command histories, security alerts, and safety events shall rely on authenticated and synchronized time sources to preserve forensic admissibility and ensure trustworthy cross-domain correlation across IT, OT, and mission systems. At this level, network time functions as a mission integrity primitive, ensuring that adversaries cannot obscure activity, manipulate sequencing, disrupt abort logic timing, or degrade detection fidelity through time manipulation.
NET-13	Enforce switch-level port security across IT, OT, security monitoring, and management fabrics to prevent unauthorized device attachment that could enable rogue device insertion (T1091) or local MITM staging (T1557.002). Configure MAC address binding with strict per-port limits and automatically shut down or quarantine ports when violations occur. Disable all unused switch ports and assign them to non-routable “dead VLANs.” Integrate port enforcement with NAC where feasible to ensure only authorized consoles, engineering laptops, OT controllers, and security appliances may attach. Monitor switch logs for port violations and forward events to the SOC for review. Include port lockdown validation during mission rehearsals and pre-launch readiness activities to ensure operational procedures are understood. At this level, port security provides controlled prevention of rogue device attachment and basic containment of unauthorized physical insertion attempts within mission networks.	Implement certificate-bound device authentication using 802.1X with EAP-TLS to cryptographically bind device identity to switch ports across IT, OT, security monitoring, and management networks. Automatically quarantine unauthorized or anomalous devices with real-time SOC alerting. Continuously monitor for MAC spoofing, ARP poisoning, and inline tap behavior using anomaly detection tied to switching telemetry. Integrate port security events with physical security systems so rogue port activity triggers on-site investigation during mission-critical operations. Enforce tamper-evident, immutable logging of all port violations for forensic reconstruction. Conduct red-team rogue device injection exercises to validate that insider or physical insertion attempts into security racks, ICS/OT stacks, or management fabrics are detected and contained before enabling lateral movement or traffic interception. At this level, port security becomes identity-bound, continuously monitored, and operationally integrated with physical and cyber response workflows to prevent and rapidly contain insider or rogue-device compromise of trusted network zones.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-14	The network shall implement VLANs, internal firewalls, and routed boundaries to separate operator consoles, C2 workstations, antenna controllers, OT PLCs, fueling systems, mission management systems, and enterprise IT. The mission shall also adopt a Purdue-like network architecture for ICS/OT environments, establishing clear trust boundaries between enterprise IT, supervisory OT, and field control systems. Default-deny communication policies shall be enforced between segments, allowing only explicitly authorized mission-required traffic (e.g., uplink command paths, telemetry ingest flows, safety monitoring feeds). Isolate antenna control, RF management, time authority, storage systems, security services, and DCO infrastructure from unrelated mission or enterprise systems to limit lateral movement and reduce MITM exposure (T1557, T1210, T1190). Prevent direct partner or enterprise access to mission-critical enclaves. Isolate ingestion, processing, analytics, archives, and distribution tiers to limit data manipulation and pivot opportunities (T1565). Separate launch control networks and fueling systems from adjacent mission networks to prevent compromise from cascading during critical operations (T1498, T0820). Regularly review segmentation policies against operational needs. Validate segmentation during rehearsals by simulating compromised nodes to ensure containment works as designed. Maintain updated segmentation diagrams and integrate them into SOC workflows for use during incident response. At this level, segmentation provides structured enclave isolation that limits lateral movement, reduces blast radius, and prevents enterprise or partner compromise from directly impacting mission-critical IT/OT systems.	Implement Zero Trust micro-segmentation where each system communicates only with explicitly authorized peers using identity-aware enforcement. Eliminate broad VLAN trust assumptions in favor of granular allowlists enforced by next-generation segmentation controls. Mandate cryptographic attestation of segmentation enforcement devices (firewalls, SDN controllers, policy engines) prior to deployment. Continuously validate segmentation policies against a golden baseline using automated compliance scanning and network modeling tools. Tie segmentation enforcement into mission readiness gates, where segmentation drift or policy failure can halt operations until corrected. Require immutable logging of segmentation policy enforcement and changes for audit and post-incident reconstruction. Conduct adversary emulation exercises specifically designed to test lateral movement attempts between IT and OT domains, partner ingress points, DCO infrastructure, and launch control networks. Validate that compromise of one enclave cannot pivot into safety systems, fueling controllers, crypto infrastructure, or spacecraft command paths. At this level, segmentation becomes identity-driven, continuously validated, and mission-enforced, providing micro-containment of compromised systems and preventing cross-domain lateral movement even under active adversary conditions.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-15	SNMP shall be restricted to SNMPv3 with strong authentication and encryption enabled. SNMPv1 and SNMPv2c shall be disabled across all routers, switches, firewalls, OT network devices, monitoring platforms, and management appliances. SNMP access shall be limited to authorized management networks and explicitly approved source IP addresses. Community strings shall not be used. All devices with SNMP enabled shall be documented, and configurations shall be reviewed quarterly and prior to mission-critical operations. SNMP activity shall be logged and forwarded to centralized monitoring systems. Alerts shall be generated for anomalous query patterns, unauthorized source attempts, or unexpected write operations. Where supported, SNMP write capabilities shall be disabled unless explicitly required for operational use. At this level, SNMP is limited to authenticated and encrypted monitoring functions, reducing reconnaissance exposure and preventing unauthorized device manipulation.	SNMPv3 shall use certificate-based authentication with per-user or per-role authorization controls enforcing least-privilege access to specific Management Information Base (MIB) objects. SNMP shall be disabled entirely on devices that do not require active monitoring. Network enforcement boundaries shall detect and automatically block attempted SNMPv1 or SNMPv2c traffic. SNMP logs shall stream in real time to SIEM/SOC pipelines with behavioral analytics to detect abnormal query volume, enumeration of sensitive OIDs, configuration write attempts, or lateral pivoting behavior. Enabling new SNMP MIBs or write access on OT devices during mission-critical windows shall require dual approval. Continuous configuration compliance validation shall ensure only approved SNMP configurations remain active. Suspicious SNMP activity shall trigger automated containment actions where operationally appropriate. Adversary emulation exercises shall validate that SNMP cannot be leveraged to enumerate, reconfigure, or pivot into mission OT, network enforcement, or defensive infrastructure systems. At this level, SNMP functions as a tightly controlled, identity-bound monitoring mechanism that prevents reconnaissance and configuration abuse while preserving mission observability.
NET-16	All trunk ports shall be configured with explicit VLAN allow-lists permitting only mission-required VLANs. Dynamic trunk negotiation (e.g., DTP) shall be disabled. Native VLANs shall not carry mission-critical traffic and shall not be used for user or OT segments. VLAN tagging consistency shall be enforced across all mission sites, including uplink facilities, launch complexes, and remote ground stations. Trunk configurations shall be audited during major milestones and prior to mission-critical operations. Unexpected VLAN tags, double-tagged frames, or anomalous trunk traffic patterns shall be monitored through network telemetry, traffic captures, or intrusion detection capabilities. Personnel shall be trained to recognize trunk misconfigurations and VLAN drift as potential adversary footholds. At this level, trunking is tightly constrained to prevent accidental mis-segmentation and reduce the feasibility of VLAN hopping or unintended cross-enclave access.	Trunk configurations shall be continuously validated against approved golden baselines using automated compliance monitoring tools. Unauthorized or drifted trunk configurations shall trigger alerts and require formal remediation. Per-trunk anomaly detection shall monitor for rogue VLAN tags, double-tagging attempts, unexpected VLAN additions, or tagging inconsistencies indicative of VLAN hopping or traffic injection attempts. Modifications to trunk configurations during mission-critical windows shall require dual approval and documented change control. Trunk telemetry shall integrate into SOC correlation pipelines to detect VLAN injection attempts aligned with lateral movement, MITM positioning, or data manipulation behaviors. Immutable logging shall record all trunk configuration changes, including user identity, timestamp, and before/after states. Red-team adversary emulation shall validate resilience against VLAN hopping, mis-tagging exploitation, and segmentation bypass attempts. At this level, trunking controls function as a segmentation enforcement mechanism that prevents cross-enclave traffic manipulation and protects mission trust boundaries from VLAN-based pivoting attacks.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-17	Remote management access is inherently higher risk than locally controlled administrative access and shall not be considered the default operating model. It shall be permitted only where mission-essential, formally authorized, and technically constrained. When activated, remote management access to routers, switches, firewalls, VPN appliances, relay switches, converters, RF bridges, and launch control network devices shall be limited to mission-essential administrative functions only. All remote logins shall require multi-factor authentication and shall occur exclusively through hardened jump hosts or bastion systems. Insecure management protocols (e.g., Telnet, HTTP, legacy management services) shall be disabled. All remote administrative sessions shall use encrypted protocols (e.g., SSHv2, HTTPS with strong cipher suites). Access shall be restricted to approved management networks and authorized source addresses. All administrative activity shall be logged, including command execution, configuration changes, authentication attempts, and session initiation/termination events. Logs shall be reviewed regularly and integrated into centralized monitoring systems. At this level, remote management access is restricted, encrypted, and auditable, reducing exposure of high-value management planes to credential abuse and remote service exploitation.	Remote management access shall be treated as an exceptional, risk-elevated activity and shall be tightly governed, time-bound, and continuously monitored, with technical enforcement preventing persistent or unmanaged administrative exposure. When activated, remote management interfaces shall be isolated on dedicated out-of-band (OOB) management networks logically and physically separated from mission, enterprise, and OT operational traffic. Mutual TLS shall be enforced for management plane access where technically feasible. All privileged sessions shall be subject to session recording, continuous behavioral monitoring, and anomaly detection capable of identifying unusual commands, abnormal login timing, configuration drift, or privilege misuse patterns. Just-in-time administrative access shall be enforced with automatic privilege revocation after task completion. Administrative access during mission-critical windows shall require formal approval workflows and time-bound authorization. Anomalous management activity shall generate real-time alerts to SOC pipelines for correlation with endpoint, firewall, and application telemetry. Red-team adversary emulation shall validate resilience against compromise of remote management interfaces, credential abuse, remote service exploitation, and management-plane pivoting attempts. At this level, remote management access functions as a hardened, continuously monitored trust boundary that prevents credential-only takeover of network infrastructure and limits the feasibility of management-plane compromise during mission-critical operations.
NET-18	All outbound internet traffic shall be routed through a secure web proxy that enforces URL filtering, TLS inspection where permitted, and malware scanning of web content and downloads. Direct internet connections from mission systems, management networks, and operator consoles shall be blocked unless explicitly authorized. Proxy policies shall restrict access to high-risk categories such as anonymizers, file-sharing platforms, and newly registered domains, and shall enforce authentication to associate activity with named users or devices. Proxy logs shall be retained per mission policy and reviewed as part of routine security operations. At this level, the web proxy functions as a centralized outbound control point, reducing opportunistic data exfiltration and providing visibility into abnormal or unauthorized web-based communications.	Direct internet connections from mission systems, management networks, and operator consoles shall be blocked unless explicitly authorized. When required, outbound web access shall be enforced through a next-generation secure web gateway providing full TLS inspection (where legally and operationally appropriate), sandbox detonation of downloaded content, contextual Data Loss Prevention (DLP) integration, and real-time threat intelligence feeds. Access policies shall be adaptive and role-aware, permitting vendor portal access, update services, or mission-support sites only to explicitly authorized personnel and systems. Geo-IP restrictions, newly registered domain blocking, and reputation-based filtering shall be enforced in near real time. All proxy telemetry shall stream continuously to SOC pipelines for correlation with endpoint, identity, and mission telemetry data. At this level, the web proxy operates as a Zero Trust egress enforcement mechanism, significantly constraining command-and-control channels and exfiltration pathways while enabling rapid detection of abnormal outbound activity during mission-critical operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
NET-19	Wireless networking shall be considered non-preferred for mission environments and shall only be deployed where mission-essential. Where wireless is permitted (e.g., enterprise or guest access zones), WPA3-Enterprise with 802.1X authentication shall be enforced. Guest wireless networks shall be fully isolated from mission and OT enclaves using dedicated VLANs and firewall boundaries. All wireless-connected devices shall pass Network Access Control (NAC) posture checks prior to gaining access. Rogue access point detection shall be enabled, and wireless logs shall feed centralized monitoring systems. At this level, wireless access is tightly controlled and segregated, reducing opportunistic entry points and limiting exposure to sniffing, man-in-the-middle, or unauthorized access attempts.	Wireless connectivity shall be prohibited within mission, OT, launch control, fueling, antenna control, and spacecraft command enclaves. Where wireless exists in enterprise or guest zones, continuous Wireless Intrusion Detection/Prevention (WIDS/WIPS) shall monitor for rogue access points, unauthorized associations, de-authentication attacks, and anomalous signal behavior. Wireless traffic shall be micro-segmented and prevented from reaching mission enclaves under all conditions. Wireless security events shall be correlated with physical access control logs and SOC monitoring pipelines to detect coordinated intrusion attempts. Periodic red-team wireless assessments shall validate isolation and resistance to rogue device insertion, credential capture, and traffic interception. At this level, wireless risk is either eliminated from mission enclaves or continuously monitored and constrained, preventing it from becoming a covert ingress path into sensitive ground or launch infrastructure.
CND-1	Standardized forensic tools & procedures shall be established for capturing volatile and non-volatile data from operator workstations, mission servers, telemetry processors, C2 systems, storage platforms, and OT endpoints. Procedures shall enable preservation of memory images, disk artifacts, configuration states, command logs, telemetry archives, CCSDS packet captures, and authentication records without unnecessarily halting mission-critical operations such as launch campaigns or active spacecraft contact windows. Forensic collection methods shall ensure integrity through cryptographic hashing and documented chain-of-custody controls. Responders shall be trained in handling mission-specific artifacts to support correlation and post-incident reconstruction. A validated forensic toolkit with integrity-verified binaries shall be staged at each operational site, and evidence shall be stored in protected, access-controlled repositories resistant to tampering or unauthorized deletion. At this level, digital forensics capability supports reliable post-incident reconstruction of attacker activity, including log tampering, data manipulation, and deletion attempts associated with T1070 and T1565, while preserving mission continuity.	Forensic readiness shall be implemented as a continuously enabled capability across IT and OT environments. All mission-relevant systems shall generate cryptographically signed, time-synchronized logs to ensure evidentiary integrity even if adversaries attempt manipulation or selective deletion. Automated evidence collection pipelines shall support rapid preservation of volatile data during incident declaration, securely transferring artifacts into isolated forensic repositories protected from operational compromise. Hardware-based write blockers, dedicated forensic networks, and offline malware analysis laboratories shall be available to analyze compromised systems without contaminating production enclaves. Storage systems, telemetry archives, configuration repositories, and command history databases shall be treated as evidentiary assets, with validated procedures to reconstruct data corruption, manipulation, or destructive activity, including scenarios aligned with T1485, T1565, and related evasion techniques. Quarterly forensic readiness exercises shall simulate mission-relevant attack scenarios such as spacecraft command injection, telemetry manipulation, or OT tampering to validate preservation, integrity validation, and reconstruction workflows. Forensic preservation steps shall be formally embedded within incident response playbooks and milestone checklists, including launch and high-risk operational windows. At this level, digital forensics functions as a mission-assurance capability that preserves evidentiary integrity under adversarial conditions, enables trustworthy reconstruction of complex IT/OT compromise scenarios, and prevents attackers from successfully erasing or falsifying the operational record.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-2	Proactive threat hunting shall be conducted within SIEM and SOC environments using hypothesis-driven methodologies aligned to relevant SPARTA and ATT&CK TTPs. Hunts shall at a minimum evaluate indicators of spoofed command activity, unusual protocol usage, anomalous RF behavior, unauthorized administrative activity, and abnormal authentication patterns associated with Valid Accounts (T1078), Masquerading (T1036), and Data Manipulation (T1565). Hunting activities shall leverage telemetry from both IT and OT sources (e.g., Windows event logs, Linux audit logs, PLC and SCADA logs, antenna control systems, RF anomaly detectors, telemetry ingest pipelines, DNS/DHCP activity, and storage access logs). Special attention shall be given to stealthy behaviors such as abnormal access volumes, permission changes, snapshot deletion, DNS abuse, and low-and-slow tunneling techniques that evade signature-based detection (T1499, T1485). Hunt results shall be formally documented, including hypotheses, data sources queried, findings, false positives, and recommended detection improvements. Findings shall feed directly into detection engineering workflows to improve alert fidelity and close observed visibility gaps. At this level, threat hunting provides structured, hypothesis-driven analysis that supplements automated detection and increases the likelihood of identifying adversaries abusing valid credentials, manipulating mission data, or staging denial-of-service conditions before operational impact occurs.	Dedicated threat hunting teams shall be established with authority to conduct deep analytical review across mission-critical enclaves during approved windows, including quiet operational periods prior to launch campaigns. Hunts shall include at a minimum adversary emulation scenarios focused specifically on space-relevant TTPs such as uplink manipulation attempts, OT pivoting from enterprise IT, abnormal launch network access patterns, and command-path abuse aligned with T0814, T1498, and T1565. Advanced analytics, including machine learning models and User and Entity Behavior Analytics (UEBA), shall be used to identify living-off-the-land behaviors on operator consoles and engineering workstations that may not trigger traditional signature alerts. Hunt cycles shall intensify prior to launch windows and following mission anomalies, with sprint-based analysis periods to proactively identify latent compromise. Hunt findings shall be correlated directly into mission readiness assessments and risk posture briefings. Where suspicious activity is identified, escalation and containment procedures shall be triggered without waiting for confirmed impact. At this level, threat hunting functions as an anticipatory defense mechanism, actively seeking stealthy or mission-specific adversary behavior within both IT and OT domains, reducing dwell time and strengthening mission assurance prior to high-impact operational events.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-3	Mission cyber defense teams shall subscribe to space-relevant threat intelligence sources, including SPARTA-aligned TTP updates, ATT&CK (Enterprise and ICS) mappings, Space ISAC bulletins, vendor advisories, and CVE feeds relevant to mission infrastructure (T1190, T1210). Indicators of compromise (IOCs), adversary infrastructure data, and TTP mappings shall be evaluated and applied to SIEM detection rules, EDR policies, DNS filtering systems, web proxies, and firewall blocklists. Known malicious domains, IP addresses, hashes, and behavioral indicators shall be reviewed and updated at least monthly or more frequently during heightened threat conditions. Threat intelligence shall be used to tune authentication monitoring and access policies (e.g., credential abuse - T1078). DNS intelligence feeds shall support identification of malicious domains and DNS-based C2 patterns (T1071.004), while recognizing that intelligence feeds supplement but do not replace behavioral detection. Validated intelligence findings shall be shared with appropriate partners using standardized formats such as STIX 2.1 and TAXII where applicable. Quarterly intelligence briefings shall be conducted for mission operators and administrators to ensure awareness of relevant adversary tactics, anti-forensic behaviors (T1027, T1036), and data manipulation techniques (T1565). At this level, threat intelligence enhances situational awareness and strengthens detection posture by aligning defensive controls with known adversary behaviors relevant to space and ground mission environments.	Threat intelligence ingestion shall be automated into SIEM, EDR, network monitoring, and endpoint protection platforms. Intelligence shall be normalized into structured formats (e.g., STIX 2.1) to enable automated correlation, enrichment, and cross-domain analytics. Intelligence shall be enriched with mission-specific context prior to operational deployment. For example, spoofed command IOCs shall be mapped to actual command dictionary entries, telemetry parameters, ground station identifiers, or RF characteristics relevant to the specific mission architecture. This contextualization shall ensure that intelligence is operationally actionable rather than generically applied. Dedicated threat-intel-to-detection pipelines shall convert newly identified adversary behaviors into detection rules, hunting queries, or preventive controls within defined timelines (e.g., within 24 hours for high-confidence intelligence). Intelligence efficacy shall be continuously evaluated by comparing feed-derived detections against hunt findings, incident response data, and false-positive rates. Joint intelligence fusion exercises shall be conducted with government and industry partners to validate information sharing processes and to stress-test defensive posture against emerging space-specific TTPs. Intelligence sources shall be evaluated for integrity and reliability to reduce susceptibility to poisoned or manipulated feeds (T1565, T1584). At this level, threat intelligence functions as a continuously integrated, mission-tailored capability that rapidly translates emerging adversary behaviors into detection, prevention, and hunting actions across IT and OT mission domains, strengthening proactive defense prior to and during critical mission operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-4	Intrusion Detection and Prevention Systems (IDS/IPS) shall be deployed at mission-critical network choke points, including command uplink gateways, telemetry ingestion interfaces, planning enclave boundaries, VPN termination points, DNS/DHCP infrastructure, and other externally exposed or high-value segments. These systems shall at a minimum be configured to detect exploitation attempts against portals and remote services (T1190, T1210), adversary-in-the-middle activity (T1557), anomalous VPN or SSH behavior (T1078, T1021, T1133), and denial-of-service precursors (T1498, T1499). Signatures and detection logic shall be tuned for space- and perform mission-specific protocol decoding (e.g., CCSDS TM/TC/AOS/CFDP/SLE) for any custom telemetry or command formats. IDS capabilities shall at least monitor for command stream corruption, unauthorized ephemeris injection, relay abuse, malformed commands, and protocol manipulation attempts (T1565). ICS-aware IDS functionality shall be enabled where applicable to detect abnormal command sequences or unsafe field network interactions in environments where native authentication is limited (T0814, T0855). Inline IPS enforcement shall be enabled in high-risk zones such as internet-facing portals and remote access VPN infrastructure. IDS/IPS alerts shall be reviewed daily, and rule tuning shall be conducted at least monthly to reduce false positives and ensure coverage of mission-relevant traffic patterns. IDS telemetry shall be forwarded to centralized SIEM systems for correlation with endpoint, authentication, and operational telemetry events. At this level, IDS/IPS provide foundational visibility into exploitation attempts, protocol abuse, command manipulation, and network-based denial activity across mission IT and OT domains.	Next-generation IDS/IPS platforms shall provide full protocol decoding for mission-specific traffic (e.g., CCSDS TM/TC/AOS/CFDP/SLE) and custom telemetry or command structures. Detection shall combine signature-based, behavioral, and anomaly-based techniques (statistical or machine learning models) to identify novel protocol abuse, malformed traffic, obfuscated payloads (T1027), anomalous encrypted session negotiation (T1557, T1600.002), and subtle data manipulation patterns (T1565). Inline IPS enforcement shall operate with automated blocking capabilities based on risk scoring and contextual mission phase awareness. IPS actions shall be integrated with SOC SOAR playbooks to enable automated containment actions (e.g., isolating compromised hosts, disabling suspect remote VPN/SSH/VNC sessions, or blocking malicious scheduling API traffic) (T1499, T1078). Detection rules shall be continuously updated using external threat intelligence feeds and internal hunt findings. IDS/IPS health and detection output shall be continuously validated. Unexpected gaps in alerts, sudden silence from sensors, or unexplained changes in detection patterns shall be investigated as potential defense evasion or monitoring impairment activity (T1562). IDS/IPS telemetry shall be correlated with NOC and mission telemetry systems to identify anomalies affecting command paths, telemetry integrity, time synchronization, VPN negotiations, encrypted session behavior and/or other network related anomalies. Semi-annual red-team adversary emulation exercises shall at a minimum validate detection coverage for command injection attempts, telemetry corruption, protocol tunneling (T1071.004), credential replay, and lateral movement into mission enclaves. At this level, IDS/IPS function as an adaptive, mission-aware enforcement and detection capability that actively disrupts exploitation attempts, protocol abuse, and lateral movement across ground and OT environments during routine operations and high-impact mission phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-5	Incident response procedures shall be formally documented to address items like IT malware, credential compromise, insider misuse, OT disruption, uplink manipulation, telemetry corruption, and denial-of-service conditions across mission environments. Playbooks shall define clear decision authority and response actions for Mission Operations Center (MOC), launch control, engineering teams, and ground operators, ensuring rapid containment and restoration actions for scenarios such as antenna mispointing, RF path degradation, unauthorized command execution, corrupted schedules, dictionary tampering, or telemetry integrity concerns associated with T1489, T1499, T1565, and T1078. Procedures shall explicitly define escalation thresholds, including authority to pause launch activities, isolate communication paths, revoke credentials, invalidate suspect command loads, or restore known-good configurations. Response guidance shall address service interruption, relay compromise, parameter tampering, archive corruption, and key revocation scenarios, particularly where time constraints during launch windows increase operational risk. Tabletop exercises shall be conducted prior to major mission milestones, including launch campaigns, to validate decision flow, inter-team coordination, and communication with external partners or federal authorities. Evidence preservation steps, chain-of-custody requirements, and log retention processes shall be integrated into all procedures to ensure defensible post-incident reconstruction. At this level, incident response functions as an organized containment and recovery framework that minimizes mission disruption, limits damage from credential abuse or service impairment, and enables controlled restoration of operational capability.	Incident response capabilities shall evolve into a fully integrated cyber-physical response program aligned to mission safety and launch decision authority. Response workflows shall integrate cybersecurity actions with operational decision logic, including coordinated cyber and launch-abort exercises to validate authority, timing, and communication under high-impact scenarios such as fueling operations, uplink compromise, or telemetry falsification attempts associated with T1485, T1489, T1498, and T1562. Automated containment mechanisms shall be integrated into SOAR platforms where appropriate, enabling rapid enforcement actions (e.g., ACL lockouts, credential revocation, console isolation, uplink suspension, or enclave segmentation) while preserving safety constraints. Any response action impacting safety-critical systems, cryptographic material, or launch sequencing logic shall require dual authorization during mission-critical windows. Quarterly live-fire exercises incorporating adversary emulation shall validate the ability to detect, contain, and recover from coordinated IT and OT attacks under time-constrained operational conditions. Monitoring impairment, telemetry manipulation, and loss-of-visibility scenarios shall be treated as distinct incident classes with predefined playbooks to prevent decision paralysis during degraded awareness conditions. Incident response metrics, readiness posture, and corrective actions shall be formally reviewed during mission assurance gates to ensure response capability remains aligned with evolving threat conditions. At this level, incident response functions as a mission assurance safeguard that synchronizes cybersecurity containment with physical safety controls, prevents cascading mission failure, and ensures rapid, coordinated recovery even under adversary pressure during high-impact mission phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-6	Security sensors shall be deployed at mission-critical choke points including at a minimum command uplink interfaces, telemetry ingestion paths, VPN termination points, DMZ boundaries, storage network interfaces, routing cores, and network management segments. These sensors shall capture telemetry necessary to detect anomalous command activity, malformed inputs, unexpected execution timing, unauthorized schedule modifications, relay abuse, denial-of-service precursors, and protocol manipulation attempts associated with T1565, T1498, T1499, and T1059. Sensors shall monitor antenna behavior for unexpected pointing changes, polarization mismatches, abnormal calibration activity, RF attenuation shifts, routing anomalies, amplifier shutdown conditions, and anti-jam configuration changes indicative of manipulation (T0855, T1489). Endpoint agents shall be deployed on all supported operator workstations, mission servers, analytics engines, and supported OT systems to provide process, file, authentication, and defense-evasion telemetry (T1562, T1070, T1546). Telemetry from network, endpoint, application, and cryptographic boundaries shall be forwarded to centralized SIEM/SOC platforms for correlation. Coverage shall be validated quarterly to ensure no blind spots exist across mission, launch, and OT enclaves. Storage, crypto, and management plane sensors shall capture key access events, signing activity, export attempts, and abnormal session establishment patterns to detect stealthy misuse rather than only generic malware activity (T1485, T1040). At this level, security sensors provide distributed telemetry across IT and OT environments, enabling detection of manipulation, denial-of-service, credential abuse, and defense evasion behaviors before mission impact occurs.	Security sensor coverage shall be redundant and geographically distributed to eliminate single points of telemetry failure. Multiple network vantage points shall be instrumented to enable cross-correlation and reduce the effectiveness of sensor suppression or selective blinding attempts (T1562, T1070). Full-packet capture (PCAP) shall be enabled on high-value links such as uplink paths, telemetry ingest interfaces, storage backbones, and gateway boundaries, with retention tuned to mission phase and risk posture. Tamper-resistant or physically protected sensors shall be deployed on critical uplink and launch control paths to prevent manipulation or disablement during high-impact operations. Sensor health, telemetry flow rates, and alert baselines shall be continuously monitored, and degradation in sensor coverage or anomalous silence shall trigger real-time alerts for investigation. Telemetry shall include packet-level, API-level, and application-layer data to detect replay attempts, exfiltration behaviors, encrypted session anomalies, credential misuse, and command-path manipulation (T1090, T1041, T1565). Dedicated sensors around deception and monitoring infrastructure shall provide high-fidelity insight into adversary interaction patterns even under partial evasion attempts. Annual red-team exercises shall specifically test sensor evasion techniques, telemetry suppression scenarios, replay attacks, and coordinated uplink manipulation attempts to validate detection resilience. At this level, security sensors function as a resilient, mission-aware telemetry fabric that maintains visibility across distributed ground and OT environments, preserves detection continuity under adversary pressure, and significantly reduces the feasibility of covert manipulation or monitoring impairment during mission-critical operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-7	Logs from mission servers, command and telemetry systems, planning tools, relay endpoints, crypto services, storage platforms, identity systems, network infrastructure, and supporting IT and OT components shall be centrally aggregated into a Security Information and Event Management (SIEM) platform. Anti-jam configuration changes, DSP firmware loads, uplink events, VPN sessions, crypto access events, and enclave network telemetry shall be forwarded to enable cross-domain correlation of activity associated with T1601, T1489, T1078, and T1565. Correlation rules at a minimum shall be implemented to detect anomalous command activity, malformed inputs, unexpected execution timing, unauthorized schedule changes, relay abuse, and rogue industrial protocol traffic. Correlation shall combine OS logs, TT&C logs, network telemetry, authentication events, and crypto service activity to provide unified visibility into stealthy manipulation attempts and credential misuse. The SIEM shall support dashboards tailored to mission operations, including launch windows, uplink sessions, telemetry ingest, OT controller health, and time synchronization integrity. Logs shall be retained in accordance with mission compliance requirements, with a minimum retention period sufficient to support post-incident reconstruction and regulatory review. Log integrity shall be preserved through controlled access and audit tracking. At this level, the SIEM functions as the centralized aggregation and correlation backbone for mission cyber defense, enabling detection of coordinated multi-step attacks across identity, network, endpoint, crypto, and mission telemetry domains.	The SIEM shall implement advanced analytics, including machine learning and User and Entity Behavior Analytics (UEBA), to detect subtle anomalies such as drift in operator behavior, low-and-slow exfiltration, credential replay, unusual API usage, timestamp inconsistencies, and gradual manipulation of telemetry or planning data (T1078, T1539, T1565). Correlation shall span identity systems, remote access (e.g., VPN/SSH/VNC), endpoint integrity signals, crypto events, storage activity, and network telemetry to identify coordinated attack chains. Threat intelligence feeds shall be directly integrated into correlation rules and enrichment pipelines, enabling automated contextualization of events with known adversary infrastructure, TTP patterns, and confidence scoring. Detection logic shall be continuously tuned based on red-team exercises, hunt findings, and incident response lessons learned. Logs shall be protected using cryptographic integrity controls to prevent tampering, deletion, or falsification (T1562, T1070). Automated escalation workflows shall assign risk scores and trigger SOC playbooks for containment, investigation, or launch decision support. The SIEM platform itself shall be treated as mission-critical infrastructure, with monitoring to detect ingestion failures, rule corruption, suppression attempts, or abnormal alert silence indicative of defense impairment (T1562, T1211). Quarterly rule reviews and tuning cycles shall be required, informed by adversary emulation campaigns and operational anomaly trends. At this level, the SIEM operates as a mission-assurance analytics engine, correlating cyber, network, cryptographic, and operational telemetry to identify stealthy, coordinated, or low-visibility attacks that would evade isolated security controls, particularly during high-impact mission phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-8	The Security Operations Center (SOC) shall be staffed with personnel cross-trained in space telemetry formats, TT&C systems, OT/ICS protocols, RF behavior, and traditional IT cybersecurity disciplines. SOC analysts shall understand command timing, uplink workflows, launch sequencing logic, and mission planning systems to properly interpret anomalous activity associated with T1565, T1059, and T1078. The SOC shall operate continuous monitoring during mission-critical windows, including launch campaigns, fueling operations, high-value uplink sessions, and anomaly resolution periods. Escalation playbooks shall define response authority, communication paths with Mission Operations Center (MOC) personnel, and thresholds for launch hold, uplink suspension, or enclave isolation actions. SOC dashboards shall provide integrated visibility across network, endpoint, telemetry, crypto, and identity systems to enable correlation of anomalous command activity, malformed inputs, unusual execution timing, defense evasion behaviors, and potential manipulation attempts. Human-in-the-loop review shall be maintained to detect subtle, "legitimate-looking" misuse patterns that automated systems may not flag (T1078). Mission planners and Mission Operations Center (MOC) personnel shall provide the SOC with advance notification of planned commanding activities, uplink sessions, schedule uploads, configuration changes, encryption transitions, and other mission-impacting operations. This information shall be shared with sufficient detail and timing to allow the SOC to distinguish authorized activity from anomalous or unauthorized behavior. Daily mission plans, approved change windows, and planned operational timelines shall be accessible to SOC analysts through controlled information-sharing mechanisms. SOC monitoring workflows shall incorporate mission plan context when evaluating command activity, authentication events, telemetry anomalies, or configuration changes. At this level, the SOC provides centralized monitoring and coordinated response capability, ensuring mission-relevant anomalies are interpreted correctly and escalated in time to prevent operational impact. Mission and cyber personnel share operational awareness to reduce false positives and improve detection of unauthorized command injection, manipulation, or credential abuse.	Mission-dedicated SOC capabilities shall be established for major campaigns or high-risk operations, with cyber defense personnel fully integrated alongside mission operations personnel for real-time joint response. Cyber situational awareness shall be integrated directly into mission operations displays to ensure command, telemetry, encryption, and network health are evaluated in a unified operational context. SOC operations shall incorporate automated SOAR workflows for high-severity alerts, enabling rapid containment actions such as credential revocation, ACL lockouts, uplink suspension, or isolation of compromised enclaves while preserving safety constraints. Continuous purple-team exercises shall validate SOC resilience, including response to telemetry manipulation, credential replay, monitoring impairment, and coordinated launch network attacks (T1562, T1498). SOC oversight shall include at a minimum validation of incident response actions, case system integrity, and detection logic to ensure attackers cannot suppress alerts, manipulate analysis platforms, or inject false positives to degrade confidence in monitoring systems. The SOC shall maintain authority to coordinate rapid response to encryption module failure, key compromise, or gateway abuse scenarios affecting spacecraft command paths (T1552, T1550). Mission operations and cyber defense functions shall be formally integrated through structured, recurring coordination processes. Real-time mission plans, command dictionaries, operational timelines, and approved deviations shall be synchronized with SOC monitoring systems to provide continuous operational context. Unplanned command activity, configuration changes, encryption state transitions, uplink sessions, or schedule modifications not aligned with declared mission operations shall be automatically flagged for investigation. SOC dashboards shall dynamically reflect current mission phase to enable phase-aware alert prioritization. Cyber situational awareness shall be incorporated into mission operations displays, and mission operations leadership shall include SOC representation in daily planning cycles and critical decision gates. Absence of declared operational activity during observed command execution or parameter modification shall be treated as a potential indicator of compromise until validated. At this level, the SOC functions as an integrated mission defense capability, synchronizing cyber detection, operational decision-making, and automated containment to preserve mission continuity during adversarial activity and high-impact operational phases. Cyber defense and mission operations function as a unified operational capability, ensuring that legitimate mission activity is clearly differentiated from covert manipulation or unauthorized command behavior during all mission phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
CND-9	Hardware Test Access Points (TAPs) shall be deployed at mission-critical network interfaces, including at a minimum command uplink paths, telemetry ingestion interfaces, launch control networks, relay endpoints, and management plane boundaries. TAPs shall provide passive, lossless copies of traffic flowing through TT&C systems and associated ground infrastructure to enable independent monitoring and packet-level inspection (T1565, T1059). TAP output shall feed IDS/IPS platforms, packet capture systems, and centralized monitoring pipelines to support detection of command manipulation, replay attempts, protocol abuse, and denial-of-service activity (T1498). Where physical TAP deployment is not technically feasible, virtual TAPs or equivalent monitoring mechanisms shall be implemented with documented limitations and risk acceptance. TAP configurations and coverage shall be validated at least quarterly to confirm correct placement, traffic fidelity, and continuous data forwarding. TAPs supporting ICS/OT or launch environments shall provide visibility into mission-critical traffic paths to detect anomalous command or control manipulation attempts (T0814). At this level, TAPs provide reliable, independent visibility into mission traffic flows, reducing reliance on switch-based monitoring and enabling detection of packet-level manipulation and protocol abuse.	Full-fidelity TAP coverage shall be implemented across all mission-critical links, including at a minimum uplink command paths, telemetry distribution backbones, launch control networks, storage backbones, VPN termination points, and management networks. TAPs shall provide lossless, tamper-resistant traffic copies independent of switching infrastructure to preserve monitoring visibility even if adversaries manipulate SPAN configurations, disable logging, or overload inline monitoring systems (T1562). TAP devices deployed on critical paths shall be tamper-resistant and utilize validated cryptographic mechanisms where applicable to ensure integrity of exported traffic data. TAP telemetry shall stream into SIEM and SOC analytics pipelines in near real-time to support rapid detection and correlation. Automated validation mechanisms shall continuously confirm TAP operational status, traffic continuity, and coverage completeness. Any degradation in TAP visibility, unexpected silence, or configuration drift shall trigger immediate investigation as a potential monitoring impairment event. Annual red-team exercises shall attempt to bypass monitoring visibility, suppress telemetry, or manipulate traffic flows to validate that TAP deployment effectively prevents blind spots in mission-critical communication paths. At this level, TAP infrastructure functions as an independent, resilient visibility layer that preserves packet-level insight across mission command, telemetry, OT, and management networks, ensuring adversaries cannot silently manipulate traffic without detection.
PER-1	Web Application Firewalls (WAFs) shall be deployed in front of all mission-facing web applications, including dashboards, telemetry status portals, scheduling tools, APIs, and operator interfaces exposed to enterprise or external networks. WAF enforcement shall require TLS 1.2 or higher with strong cipher suites, HTTP Strict Transport Security (HSTS), and centralized certificate lifecycle management. WAF rule sets shall be configured to detect and block SQL injection, cross-site scripting (XSS), command injection, deserialization attacks, authentication abuse, and other OWASP Top 10 application-layer threats aligned with T1190. Positive security models shall be implemented where feasible, permitting only expected request patterns, parameter structures, and API behaviors. Rate limiting, API exposure control, and request size constraints shall be enforced to mitigate application-layer denial-of-service attempts (T1499) and prevent dashboard manipulation or defacement (T1491). All blocked and anomalous requests shall be logged and forwarded to the SOC for correlation with authentication, endpoint, and network telemetry. At this level, the WAF functions as an application-layer inspection and enforcement control that reduces exposure of forward-facing mission portals to exploitation, injection, defacement, and volumetric abuse.	The WAF shall function as a primary application trust boundary for all mission web portals and APIs. TLS 1.3 shall be enforced with strict cipher allowlists and mutual TLS between the WAF and backend services to prevent unauthorized service-to-service access. Per-route authorization policies shall be enforced at the WAF layer, restricting access to sensitive telemetry feeds, scheduling endpoints, command preview interfaces, or administrative APIs based on role and mission phase. Attribute-Based Access Control (ABAC) or policy decision points shall be integrated directly into the WAF enforcement layer to ensure contextual authorization decisions. Session management shall be replay-resistant, and WAF-generated logs shall be cryptographically protected to prevent tampering (T1562, T1070). The WAF shall integrate with threat intelligence and SIEM correlation pipelines to dynamically adjust protections against emerging exploitation techniques. Red-team validation shall be conducted prior to major launch campaigns or mission milestones to test WAF resilience against injection attempts, bypass techniques, authentication abuse, API manipulation, and application-layer denial-of-service scenarios. At this level, the WAF operates as a mission-aware application security enforcement boundary, actively preventing exploitation, manipulation, and denial-of-service attempts against critical web-facing mission systems during routine and high-impact operational phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PER-2	Remote access into mission, planning, security, or management environments shall be considered higher risk than locally controlled access and shall not be treated as a normal or continuously enabled operating condition. Remote connectivity shall be permitted only where mission-essential and formally authorized. Where remote access is required, it shall be provided exclusively through approved VPN gateways using TLS or IPSec tunnels with strong, validated cryptographic configurations. Multi-factor authentication shall be required for all remote access accounts, with hardware-backed tokens preferred for privileged or mission-impacting roles. Device posture validation shall be enforced prior to granting access, including verification of patch level, endpoint protection status, and configuration compliance. VPN concentrators shall be deployed within controlled DMZ environments logically separated from OT networks, launch control systems, and mission-critical enclaves. Remote access to command and control (C2), planning consoles, telemetry systems, or security tooling shall be restricted to mission-essential use cases and continuously monitored for anomalous behavior indicative of attacks like credential abuse, session hijacking, or adversary-in-the-middle activity (T1078, T1550, T1557, T1563). All VPN session start, stop, and authentication events shall be logged and forwarded to centralized SOC systems for correlation with endpoint, network, and mission telemetry. At this level, remote access is tightly controlled and encrypted, reducing exposure to unauthorized ingress while preventing persistent or convenience-based connectivity into mission environments.	Remote access into mission-critical environments shall be treated as an exceptional, time-bound activity rather than a routine administrative practice. Persistent or always-available remote connectivity into C2, launch control, OT, or crypto environments shall not be permitted unless explicitly justified and approved at appropriate mission authority levels. Where technically feasible, Zero Trust Network Access (ZTNA) shall replace traditional network-wide VPN access, limiting remote users to explicitly authorized applications and services rather than broad network segments. Mutual certificate-based authentication shall be required, with device identity cryptographically bound to hardware-backed trust anchors (e.g., TPM or equivalent attestation mechanisms). Remote access shall be strictly aligned with mission phase requirements, including just-in-time access windows tied to launch campaigns, anomaly resolution periods, or scheduled maintenance. Remote sessions shall be brokered through hardened jump hosts that record administrative activity and enforce session isolation. Real-time risk scoring shall evaluate session behavior, login timing, command patterns, and authentication anomalies, triggering automated containment actions where necessary. All VPN and remote access logs shall be cryptographically protected and retained in immutable storage to support after-action review and forensic reconstruction (T1562, T1070). Quarterly red-team exercises shall validate resistance to credential replay, session hijacking, VPN gateway exploitation, and unauthorized lateral movement attempts (T1133, T1556, T1078). At this level, remote access is treated as a tightly governed contingency capability, enabling mission support when required while preventing it from becoming a persistent attack surface during routine or mission-critical operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PER-3	Outbound Internet access from mission, planning, crypto, storage, and security enclaves shall be considered non-essential by default and shall be restricted wherever operationally feasible. Direct Internet egress from OT, launch control, command uplink, and mission-critical enclaves shall not be permitted unless explicitly justified and authorized. Where outbound Internet access is required, all egress traffic shall be routed through controlled perimeter inspection points with Data Loss Prevention (DLP) enforcement enabled. DLP controls shall inspect outbound email (if applicable), web uploads, API transfers, file transfers, and removable media activity to detect unauthorized export of sensitive mission data. DLP policies shall identify ITAR-controlled information, mission data fingerprints, command dictionaries, telemetry formats, encryption material, logs, configuration exports, and other sensitive artifacts associated with T1041 and T1552. Detection logic shall include pattern matching, file fingerprinting, and threshold-based monitoring. During mission-critical windows, DLP policy violations involving mission or operational data shall trigger immediate SOC notification and documented investigation procedures. DLP telemetry shall be integrated into SIEM pipelines for correlation with identity, endpoint, and network events. At this level, outbound data flows are restricted by default and monitored when permitted, reducing opportunistic exfiltration risk and increasing visibility into unauthorized transmission of mission-sensitive artifacts following compromise.	Outbound Internet connectivity from mission and OT enclaves shall be eliminated wherever technically feasible. Where business or mission support requirements necessitate Internet access, egress shall be explicitly allow-listed, application-restricted, and continuously monitored. Adaptive DLP capabilities shall be integrated with UEBA and identity telemetry to detect insider misuse, staged exfiltration, covert data leakage, and adversary-controlled export activity aligned with T1041 and T1078. Inline DLP enforcement shall operate at egress firewalls and DMZ boundaries to prevent direct exfiltration from OT, MOC, crypto, and storage enclaves. Exports of mission-critical datasets, command archives, telemetry products, encryption material, or operational planning artifacts shall require multi-person approval workflows during defined mission phases. Cryptographic watermarking or provenance tagging shall be applied to sensitive datasets where technically feasible, and outbound flows shall be scanned for unauthorized distribution of marked content. Outbound traffic to newly registered domains, anonymization services, unsanctioned cloud storage, or non-mission geographies shall be blocked or escalated for review. DLP controls shall be validated prior to major mission milestones through adversary emulation exercises to confirm detection and prevention effectiveness. At this level, outbound Internet access is minimized, tightly governed, and continuously inspected, significantly constraining covert exfiltration pathways and reducing the likelihood that mission data leaves controlled environments without detection or authorization.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PER-4	Externally reachable services, including web portals, identity and access management systems, VPN concentrators, APIs, file transfer services, and partner connectivity nodes, shall be deployed within dedicated Demilitarized Zones (DMZs). These DMZs shall be logically and physically separated from core mission networks (e.g., areas that include sequencing systems, command uplink interfaces, telemetry ingestion platforms, storage systems, and OT control environments). Firewalls shall enforce a default-deny policy between zones, allowing only explicitly approved protocols and mission-required flows. Partner-facing services and externally accessible visualization tools shall be isolated from internal telemetry, command, and control systems to limit exposure from Public-Facing Application exploitation and remote service abuse (T1190, T1210). Zone boundaries, permitted flows, and routing paths shall be formally documented and reviewed prior to each major mission milestone or launch campaign. Activity within DMZs shall be correlated with SOC monitoring pipelines to detect probing, lateral movement attempts, authentication abuse, and anomalous partner access patterns (T1199). At this level, DMZs provide structured isolation of externally reachable services, reducing direct exposure of mission-critical systems and limiting blast radius in the event of public-facing exploitation.	A multi-tiered security zoning architecture shall be implemented, including an outer DMZ for public-facing and partner-accessible services, an inner DMZ for semi-trusted mission partners or integration environments, and protected core OT and mission enclaves separated by multiple independent enforcement layers. All zone boundaries shall be monitored by IDS/IPS platforms with protocol-aware inspection to detect cross-zone exploitation, manipulation attempts, and anomalous traffic flows. One-way data transfer mechanisms (e.g., data diodes) shall be deployed for telemetry distribution or other unidirectional mission flows where technically feasible to eliminate inbound attack paths. Firewall and zone enforcement rules shall undergo cryptographic integrity validation prior to launch readiness checks to ensure segmentation policies have not been altered or weakened. Zone configurations shall be treated as mission-critical enforcement controls and continuously monitored for drift or unauthorized modification. Red-team campaign rehearsals shall include DMZ escape attempts, cross-zone pivot scenarios, partner ingress exploitation, and API abuse exercises to validate that security zones effectively contain adversary movement (T1190, T1210, T1499, T1211). At this level, security zoning functions as a layered containment architecture that prevents externally reachable or partner-connected systems from directly exposing core mission, telemetry, uplink, or OT environments, significantly reducing the risk of lateral movement and mission-impacting compromise during routine and high-risk operational phases.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PER-5	Next-Generation Firewalls (NGFWs) shall be deployed at all mission ingress and egress boundaries, including connections to partner networks, enterprise IT, internet-facing services, and external RF or gateway environments. Firewalls shall enforce strict IP, port, and protocol allow-listing, permitting only explicitly documented and mission-approved traffic flows (e.g., CCSDS links, approved partner VPN tunnels, telemetry distribution paths). Inbound exposure shall be minimized, and geo-IP or region-based restrictions shall be applied where operationally appropriate to reduce attack surface against externally reachable services (T1190, T1210). Perimeter firewalls shall enforce rate limiting and ingress filtering to reduce exposure to volumetric and application-layer denial-of-service attempts targeting things like scheduling interfaces, command APIs, or telemetry distribution systems (T1499). Egress filtering shall be configured to constrain unauthorized outbound traffic paths that could enable exfiltration over command-and-control channels (T1041, T1048). Intrusion prevention signatures tuned for mission-relevant protocols shall be enabled at the perimeter. Firewall rule sets shall be reviewed and formally audited prior to each major mission milestone or launch campaign. At this level, perimeter firewalls function as the primary boundary enforcement layer, reducing exposure to exploitation, unauthorized ingress, denial-of-service attempts, and uncontrolled data exfiltration from mission networks.	Perimeter enforcement shall include deep packet inspection (DPI) capable of decoding mission-relevant and OT protocols (e.g., Modbus, CCSDS, proprietary launch control protocols), enabling protocol-aware validation rather than simple port filtering. Zero Trust principles shall be enforced even at the perimeter. Distinct tunnels and trust zones shall be established for different mission functions (e.g., partner payload operations vs. mission command uplink), preventing shared perimeter access paths that could enable cross-mission pivoting (i.e., multi-channel access). Real-time threat intelligence feeds shall be integrated to automatically block known malicious IP addresses, domains, and infrastructure associated with adversary campaigns. Firewall telemetry shall feed directly into SOC pipelines for behavioral correlation and rapid response. Firewall configurations shall undergo cryptographic integrity validation prior to launch readiness certification. Any rule changes during countdown or mission-critical windows shall require dual authorization and real-time SOC visibility. Red-team exercises shall include simulated exploitation of public-facing services, partner access abuse, and IT-to-OT pivot attempts to validate that perimeter controls prevent lateral movement into mission-critical enclaves (T1190, T1210, T1499, T1041). At this level, the perimeter firewall operates not merely as a filtering device, but as a mission-critical trust boundary that enforces Zero Trust segmentation, protocol-aware validation, and launch-phase stability under adversarial conditions.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PHY-1	Electronic badge systems shall be deployed for all facilities housing mission-critical systems like antenna feed systems, RF conditioning hardware, launch control rooms, operator consoles, PLC cabinets, HSMs, crypto appliances, SOC floors, DCO server rooms, and forensics labs. Badge access shall be role-based and integrated with authoritative HR identity stores. Access permissions shall reflect mission roles and be revoked immediately upon role change or separation. Anti-tailgating mechanisms shall be implemented at sensitive doorways to prevent credential sharing and unauthorized piggyback entry. Visitor badges shall be time-bound, explicitly scoped to approved areas, and require escort in mission-critical zones. Badge system logs shall be forwarded into SIEM/SOC pipelines for correlation with login events, privileged access activity, command execution, safety system changes, and OT events (T1078, T1565). Correlation between physical access and console or network activity shall be reviewed during mission-critical windows. Physical access controls shall protect against hardware implant insertion (T1200), physical tampering of RF and OT infrastructure (T0855), and console-level credential abuse (T1078, T1552). At this level, badge systems enforce controlled physical access to mission-critical computing, cryptographic modules, network infrastructure, and operator consoles, reducing the risk of hardware tampering and insider-enabled compromise.	Multi-factor physical authentication shall be required for all mission-critical areas, combining badge credentials with PIN, biometric verification, or cryptographic smartcard validation. Dual-person integrity shall be enforced for highly sensitive OT zones and launch-critical areas (e.g., fueling systems, launch sequencing rooms, crypto vaults), preventing single-individual unauthorized actions. Badge logs shall be cryptographically integrity-protected and streamed in near real time to SOC dashboards. Correlation between badge access, OT safety events, command submissions, key access operations, and security alert suppression shall be automated to detect coordinated cyber-physical activity (T1562, T1565). Access to DCO infrastructure (SIEM, SOAR, EDR backends, forensic labs) shall be treated as mission-critical, with enhanced monitoring to prevent log deletion (T1070), sensor tampering (T1562), or artifact manipulation (T1565). Red-team exercises shall include tailgating attempts, badge cloning simulations, and physical access bypass testing prior to major launch campaigns to validate resilience. At this level, physical access control becomes a fully integrated cyber-physical defense mechanism, preventing hardware-level compromise, insider abuse, and defense-blinding attempts that could directly impact launch safety and mission continuity.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PHY-2	Mission-critical computing, networking, cryptographic, storage, RF equipment, OT control racks, and launch control infrastructure shall be protected by clean-agent fire suppression systems (e.g., FM-200, Novec 1230) to prevent hardware destruction, mission data loss, and cascading system outages. Zoned smoke detection systems shall be installed in server rooms, control racks, and mission operations facilities to enable early detection of environmental anomalies. Detection sensors shall be tested quarterly, and suppression systems shall undergo regular maintenance inspections to ensure operational readiness. Fire detection and suppression alarms shall be integrated into both SOC and NOC dashboards to provide unified situational awareness across cyber, network, and environmental domains. Alerts shall be treated as mission-impacting events when occurring within facilities supporting command, telemetry, cryptographic, storage, or launch operations. Fire suppression capability shall preserve mission continuity and reduce risk of availability loss (T1498), destructive impact (T1485), or loss of visibility due to infrastructure damage (T1562). At this level, fire suppression provides essential environmental protection for mission-critical cyber and OT infrastructure, reducing the risk that environmental incidents cascade into mission-impacting outages.	Redundant, zoned fire suppression systems shall be deployed across all facilities supporting launch, fueling, command, telemetry, cryptographic key management, and OT control functions. Suppression zones shall be architected to prevent single-system failure from disabling entire mission operations areas. Very Early Smoke Detection Apparatus (VESDA) or equivalent high-sensitivity detection technologies shall be deployed for proactive anomaly detection prior to flame conditions. Where facilities are in proximity to launch pads or fueling operations, fire detection systems shall be integrated with launch abort and safety interlock systems to automatically halt fueling or other hazardous operations upon confirmed fire events. Fire suppression system status, activation events, and maintenance logs shall be cryptographically integrity-protected and retained for compliance and forensic review. Third-party certification of fire suppression readiness shall be required prior to major launch campaigns. At this level, fire suppression becomes an integrated mission-safety control that protects not only infrastructure availability but also launch safety, operational continuity, and forensic accountability in the event of environmental or sabotage-related incidents.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PHY-3	Facilities hosting mission-critical ground systems, including mission operations centers (MOC), launch control facilities, antenna sites, fueling systems, datacenters, and OT control environments, shall implement perimeter security controls including fencing, controlled gates, and vehicle barriers to prevent unauthorized physical approach. All vehicle and pedestrian access points shall require badge verification or visitor vetting prior to entry. Visitor access shall be logged and restricted to approved areas. Roaming security personnel shall be employed during operational windows, equipped with secure communications integrated with SOC and NOC monitoring channels to ensure rapid coordination during security incidents. Facilities shall conduct periodic drills simulating vehicle breach attempts or unauthorized perimeter entry to validate guard response, escalation procedures, and integration with cyber response teams. Perimeter security controls reduce the risk of sabotage, tampering, hardware implant insertion, service disruption, and insider-facilitated compromise that could cascade into cyber or mission-impacting events (T1485, T1498, T1565). At this level, perimeter security provides deterrence and early detection against physical intrusion that could enable direct hardware compromise or disruption of mission-critical systems.	High-value launch, fueling, and mission operations facilities shall maintain 24/7 armed guard presence during mission campaigns and critical operational windows. Crash-rated vehicle denial barriers (e.g., certified bollards, wedge barriers, reinforced gates) shall be deployed to protect facilities from forced vehicle entry or ramming attempts. Guard patrol routes, incident reports, and access logs shall be digitized and integrated into centralized monitoring systems, with correlation to badge access, OT alerts, and SOC activity for real-time situational awareness. Joint guard–SOC exercises shall be conducted to simulate hostile entry attempts, insider coercion scenarios, and coordinated cyber-physical attacks targeting mission infrastructure. Advanced perimeter monitoring capabilities, including UAV surveillance or AI-assisted video analytics, shall be deployed during launch campaigns to extend detection coverage beyond static fence lines. Launch windows create predictable, high-value timing for adversary action. Physical perimeter security shall therefore be treated as a mission-critical defense layer supporting resilience against sabotage, coercion, insider threats, and coordinated cyber-physical campaigns (T1498, T1485, T1562). At this level, perimeter security operates as an integrated cyber-physical defense system, providing deterrence, detection, and rapid response capabilities that directly protect mission continuity and launch safety.
PHY-4	Facilities hosting mission-critical systems, (e.g., antenna control environments, RF path components, launch control rooms, operator consoles, datacenters, OT cabinets, and cryptographic infrastructure) shall maintain auditable physical access logs recording all personnel and visitor entry and exit events. Both paper and digital visitor logs shall be time-stamped, reviewed weekly, and retained according to mission retention policies. Escort policies shall be enforced for non-cleared visitors, and escort identity shall be documented in visitor records. Physical access logs shall be correlated with badge system events to ensure consistency and detect discrepancies such as tailgating, badge misuse, or unauthorized after-hours presence. Logs shall support forensic reconstruction of events involving unauthorized commands, log tampering, safety system manipulation, hardware implant insertion, or service disruption (T1070, T1078, T1485, T1498, T1565). At this level, physical logging provides accountability and traceability for mission-critical spaces, enabling post-incident reconstruction and insider threat detection when cyber or operational anomalies occur.	Physical access logging systems shall be implemented using tamper-resistant digital platforms with immutable storage protections to prevent alteration or deletion of records. Visitor and access logs shall be streamed into SIEM/SOC pipelines for automated correlation with cyber anomalies, including command submissions, authentication events, safety system triggers, and alert suppression activity (T1562, T1565). Quarterly audits shall compare visitor logs against HR rosters, role assignments, and authorized access rights to detect unauthorized presence or privilege drift. Video verification mechanisms (e.g., CCTV snapshots tied to entry events) shall be linked to digital log entries to provide unambiguous identification of individuals entering mission-critical areas. Correlation between physical presence and mission-impacting events (e.g., launch aborts, anomalous commands, crypto key access, OT logic changes) shall be automated to detect coordinated cyber-physical activity. At this level, physical logging becomes an integrated investigative and detection control, ensuring that physical presence can be correlated in near real time with cyber events, preventing insider abuse, log manipulation, and coordinated cyber-physical attacks from escaping attribution.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PHY-5	Facilities supporting mission-critical ground systems, including launch operations, mission operations centers (MOC), antenna sites, datacenters, OT control rooms, and cryptographic infrastructure, shall maintain dedicated on-site or contracted protective personnel responsible for physical deterrence, anomaly response, and escalation. Security personnel shall be trained on mission-specific threat scenarios (e.g., sabotage attempts, insider coercion, unauthorized physical access to operator consoles, hardware tampering, and coordinated cyber-physical pivoting)(T1565, T1498, T0814). Security communications shall be integrated with SOC and NOC incident workflows to ensure rapid coordination between physical and cyber response teams. Guard observations, suspicious activity reports, and physical anomaly alerts shall be treated as mission-impacting signals during launch and other high-risk operational windows. Security personnel shall enforce procedural controls during critical mission phases (e.g., anomaly response windows, high-risk commanding periods, fueling operations, and cryptographic key handling activities). At this level, mission security personnel provide deterrence and rapid response capability against physical intrusion, insider abuse, and coordinated cyber-physical activity that could disrupt mission operations or compromise safety.	Mission-critical facilities shall maintain mission-trained security personnel with appropriate clearance and familiarity with space operations, ICS/OT environments, launch procedures, and command authority structures. Joint cyber-physical red-team exercises shall be conducted to validate coordination between security personnel and SOC teams under simulated hostile entry attempts, insider coercion scenarios, or coordinated cyber-physical campaigns. Security personnel shall be equipped with secure communications directly integrated into SOC dashboards and incident management systems to enable real-time situational awareness. Rapid-response teams shall be authorized and trained to immediately intervene in unsafe or anomalous operational conditions, (e.g., isolating fueling systems, restricting access to launch control rooms, securing cryptographic equipment, or halting physical operations when required). Launch and major mission milestones shall be treated as elevated risk states requiring heightened physical security posture and authority to intervene if abnormal behavior, coercion, or coordinated anomalies are detected (T1498, T1485). At this level, mission security personnel function as an integrated cyber-physical defense capability, providing immediate human intervention authority to prevent sabotage, insider compromise, or mission-impacting physical tampering during high-value operational windows.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PHY-6	Mission-critical facilities shall provide redundant power and communications infrastructure, including backup generators, uninterruptible power supplies (UPS), and alternate communication links for command, telemetry, cryptographic services, SOC/DCO platforms, and launch control environments. Critical utility dependencies, including power feeds, cooling systems, network backbones, and RF relay paths, shall be formally documented. Tabletop exercises shall simulate power loss, utility disruption, or communications outages to validate continuity procedures. Alternate operating procedures shall be documented for loss of primary utilities, including fallback command paths, manual coordination processes, and degraded operations workflows. Spare hardware for mission-critical systems, including networking devices, OT controllers, storage systems, and cryptographic modules, shall be maintained and inventoried to enable rapid restoration following infrastructure failure. At this level, infrastructure diversity reduces single points of failure and ensures mission operations can continue despite localized outages or physical disruptions. Infrastructure diversity supports continuity of operations and reduces mission impact from service stop, denial-of-service, destructive events, or environmental disruptions (T1489, T1499, T1485, T1562).	High-value mission operations shall be supported by geographically distributed redundant facilities, including secondary Mission Operations Centers (MOCs), SOC/DCO nodes, and command infrastructure capable of hot or near-hot failover. Automated failover drills shall be integrated into launch readiness processes to validate continuity of command, telemetry monitoring, safety interlocks, and cyber detection during simulated primary-site loss. Dual-path power feeds with real-time monitoring shall be implemented for critical facilities to reduce susceptibility to localized grid failure or sabotage. Mission exercises shall simulate full-site loss scenarios, requiring continuity of operations from secondary facilities without degradation of safety, security monitoring, or command authority. Redundancy shall extend beyond local infrastructure to enterprise-level Continuity of Operations (COOP) plans, ensuring mission continuity during widespread environmental, cyber, or physical disruption events. Redundant SOC and DCO capabilities in geographically separate locations shall prevent single-site loss from blinding detection, monitoring, or incident response capability (T1562). At this level, infrastructure diversity becomes a mission-level resilience architecture, eliminating single points of failure and ensuring sustained command, monitoring, and cyber defense capability even under catastrophic physical or cyber disruption conditions.
PHY-7	Closed-circuit television (CCTV) systems shall provide continuous visual coverage of sensitive perimeters, launch pads, fueling racks, antenna shelters, control rooms, datacenters, OT racks, cryptographic equipment areas, and other mission-critical zones. Video shall be retained for no less than 90 days, or longer where mission requirements dictate, to support forensic reconstruction of physical events associated with mission-impacting anomalies. Surveillance feeds shall be integrated into SOC monitoring environments, and daily spot checks shall be performed to verify camera functionality, coverage completeness, and recording integrity. Video monitoring shall support. at a minimum the detection and deterrence of physical interference, hardware tampering, insider misuse, and unauthorized presence in areas supporting command, telemetry, fueling, and safety systems (T0855, T1485, T1498, T1565). At this level, surveillance enhances deterrence, detection, and forensic accountability by providing visual evidence of physical activity tied to mission-critical systems.	AI-enhanced video analytics shall be deployed to detect anomalous behaviors including loitering near restricted areas, fence breaches, tampering near fuel lines or RF hardware, abnormal access patterns in control rooms, or unauthorized presence during restricted operational windows. Video storage systems shall implement cryptographic integrity protections to ensure admissibility and prevent tampering or deletion of footage during or after incidents. Surveillance alerts shall be streamed in real time to SOC dashboards and correlated with badge access, OT alarms, command activity, and network anomalies to detect coordinated cyber-physical activity. Red-team exercises shall include attempts to bypass, blind, disable, or spoof camera systems to validate surveillance resilience and detection effectiveness prior to launch campaigns. At this level, surveillance operates as an integrated detection layer within the cyber-physical defense architecture, providing real-time anomaly detection and high-confidence forensic evidence during mission-critical operations.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-1	Mission personnel (e.g., operators, engineers, launch staff, SOC analysts, and OT technicians) shall receive quarterly awareness campaigns tailored to space mission threats. Training shall address phishing targeting operators (T1566), spoofed telemetry dashboards, USB baiting at launch pads (T1204), credential harvesting, and social engineering paths that enable valid account abuse (T1078). Awareness training shall reinforce anomaly recognition specific to mission environments (e.g., unexpected antenna movements, abnormal telemetry values, unplanned OT device reboots, suspicious command sequences, or inconsistent dashboard outputs). Clear escalation channels into the SOC and NOC shall be documented and reinforced. Reporting procedures shall be incorporated into mission readiness checklists to ensure anomaly reporting is treated as part of operational discipline rather than optional behavior. Tabletop drills shall simulate cyber-physical anomaly scenarios (e.g., false fuel sensor readings, spoofed telemetry views, coordinated phishing during launch rehearsal). Reporting metrics shall be tracked, and personnel who identify and escalate anomalies shall be formally recognized to reinforce vigilance. At this level, personnel awareness builds a vigilant workforce capable of detecting and reporting early indicators of social engineering, phishing, insider abuse, and cyber-physical manipulation before adversary activity escalates into mission impact.	A continuous awareness program (weekly or monthly) shall be established, with mandatory refreshers every 6–12 months tied directly to mission readiness certification. Red-team-driven awareness drills shall be conducted during launch rehearsals and high-risk operational windows, such as simulated phishing campaigns targeting launch engineers, staged RF tampering alerts, false status dashboards, and coordinated cyber-physical anomaly injections. Metrics dashboards shall measure reporting timeliness, escalation accuracy, and anomaly recognition effectiveness. Results shall be tied to operator certification, role qualification, and mission assurance reporting. Conduct controlled anomaly injection exercises that blend cyber indicators (e.g., suspicious logins, phishing attempts) and mission telemetry irregularities (e.g., unexpected uplink activity, sensor drift, OT configuration changes) to validate operator detection and escalation performance (i.e., cyber physical purple teaming). Awareness and reporting performance shall be incorporated into enterprise performance reviews and mission assurance documentation, reinforcing that vigilance is an operational requirement. At this level, personnel awareness functions as an operational defense layer, measurably reducing susceptibility to phishing, social engineering, user execution attacks, and valid account abuse while strengthening early detection of coordinated cyber-physical campaigns.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-2	Provisioning and deprovisioning workflows shall be formally documented and directly tied to authoritative HR events, including hiring, role change, contractor onboarding, and separation. All operator, administrator, engineer, contractor, and vendor accounts associated with Mission Operations Centers (MOC), launch control environments, ground station equipment, OT PLCs, cryptographic systems, and security infrastructure shall be reviewed at least quarterly to eliminate stale, orphaned, or unnecessary accounts (T1078, T1098). Shared vendor or service accounts shall be eliminated wherever technically feasible and replaced with uniquely identifiable, named identities. Access to mission-critical consoles for things like launch sequencing systems, fueling controllers, and/or command uplink infrastructure shall require explicit manager approval for role changes or privilege elevation. Time-bound access shall be enforced for launch support personnel and integration contractors, with immediate deprovisioning following campaign completion to reduce exposure during time-compressed operational windows. Provisioning metrics, including orphaned account counts, privilege assignments, and recertification status, shall be tracked and reviewed prior to each mission campaign. At this level, personnel management reduces insider risk and the likelihood of valid account abuse by ensuring identity lifecycles are tightly governed and access is not retained beyond operational necessity.	Identity lifecycle management shall be automated with full integration between HR systems, Identity and Access Management (IAM) platforms, and SOC monitoring environments to ensure near-real-time provisioning and deprovisioning enforcement. Zero Trust identity principles shall be enforced, including just-in-time privilege elevation, continuous insider-risk scoring, and strict least-privilege enforcement for all mission-critical roles. Creation or deletion of high-value accounts (e.g., OT fueling controllers, launch sequencing consoles, cryptographic key custodians, MOC commanding roles, and subscription or quota administrators) shall require dual authorization and formal logging. All privileged roles shall undergo periodic recertification, with documented attestation of continued need and scope of authority. Identity telemetry shall be integrated into SIEM/SOC pipelines to automatically flag anomalous behavior (e.g., sudden OT access by non-OT roles, unexpected launch console access, after-hours privileged activity, or privilege escalation inconsistent with operational plans) (T1078, T1098). Deprovisioning of partner and enterprise identities shall be enforced promptly at contract expiration or role change to prevent long-lived credential risk and post-engagement abuse (T1586.002). At this level, personnel management becomes a continuously monitored identity governance control, measurably reducing insider threat exposure, orphaned account risk, and privilege abuse across mission-critical systems.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-3	All systems that enforce security boundaries, process mission data, control operational interfaces, or support launch and mission operations shall undergo regular security assessments. Quarterly vulnerability scanning shall be conducted on mission IT systems (servers, operator consoles, identity services) and supported OT/ICS devices (PLC firmware, antenna controllers, fueling control systems) where technically feasible and safe to do so. Penetration testing shall validate countermeasures like encryption implementation, role-based access controls, audit logging integrity, segmentation enforcement, and remote access protections. Mission-critical systems shall be assessed as deployed, not solely through design reviews, to identify configuration weaknesses that could enable exploitation of remote services or lateral movement (T1210, T1078). Mission-specific adversarial simulations shall be included in assessment programs, such as spoofing RF signals, attempting pivot from IT to OT networks, validating segmentation barriers, and testing detection of anomalous telemetry manipulation (T1565, T1498). Assessment findings shall be reviewed during mission readiness reviews, and corrective actions shall be tracked to closure prior to campaign execution. At this level, security assessments validate that controls function as designed under realistic threat conditions and reduce the likelihood of misconfiguration-driven compromise or undetected weaknesses in mission systems.	An annual full-spectrum red/blue team exercise shall be conducted, aligned to SPARTA and ATT&CK threat-informed scenarios, covering IT, OT/ICS, launch control, ground networks, cryptographic systems, and SOC detection pipelines. Independent third-party penetration testing shall be performed on the most critical systems and environments, including OT/ICS devices, fueling systems, launch pad control networks, uplink gateways, and mission operations infrastructure. Corrective action plans shall be formally documented and tracked. Adversary emulation shall include at a minimum advanced cyber-physical scenarios such as PLC firmware modification attempts, uplink manipulation, telemetry falsification, monitoring impairment (T1562), and credential abuse (T1078). Assessment outcomes shall be tied directly into mission risk registers, readiness gates, and launch certification criteria, ensuring that unresolved high-risk findings are explicitly adjudicated prior to mission execution. A rolling program of purple-team activities shall be maintained to rehearse detection and response against current space-relevant threat intelligence, validating that monitoring, logging, and SOC processes cannot be trivially bypassed or disabled (T1562, T1070). At this level, security assessments become an operational validation mechanism, continuously stress-testing cyber, OT, and launch systems against realistic adversary behaviors and directly informing mission risk decisions.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-4	A structured threat assessment process using SPARTA and ATT&CK frameworks shall be conducted at least quarterly to evaluate adversary motivations, capabilities, intent, and likely attack pathways against mission operations centers (MOC), ground stations, launch systems, OT/ICS environments, cryptographic services, and supporting enterprise infrastructure. Threat assessments shall leverage open-source intelligence, government threat reporting, Space ISAC products, and sector-specific advisories to identify campaigns targeting satellite operators, aerospace contractors, ground networks, and OT vendors. Analysis shall prioritize high-impact threat vectors including techniques related to credential theft and valid account abuse (T1078), public-facing exploitation (T1190), RF spoofing or signal manipulation (T0855), OT/ICS control logic abuse (T0814), monitoring impairment (T1562), and denial-of-service behaviors (T1498, T1499). Structured risk scoring shall be applied to align defensive investment with mission impact and adversary realism rather than generic IT risk assumptions. Threat assessment findings shall be shared with mission operators and incorporated into tabletop exercises, launch rehearsals, and red-team scenarios to ensure threat-informed readiness. At this level, threat assessment ensures defensive decisions are aligned to realistic adversary capabilities and mission-impacting attack paths rather than abstract or compliance-driven assumptions.	A continuous threat assessment program shall be implemented leveraging SPARTA and ATT&CK frameworks to map adversary techniques directly to mission systems, OT devices, launch infrastructure, and defensive controls. Live intelligence feeds shall be fused with structured wargaming and adversary emulation to simulate realistic campaigns targeting MOC, launch, cryptographic, and OT environments. Mission-specific adversary reports shall be delivered at least quarterly, including analysis of new TTPs targeting satellite operators, launch facilities, ground networks, and defensive monitoring infrastructure. All intelligence products shall be integrated into SOC workflows, with Indicators of Compromise (IOCs) and Indicators of Behavior (IOBs) automatically translated into detection logic, monitoring updates, and purple-team validation exercises. Threat modeling shall be used to drive funding decisions, architecture changes, segmentation priorities, monitoring enhancements, and defensive investments during mission design reviews and readiness gates. Threat assessments shall explicitly consider adversary behaviors targeting defensive infrastructure itself (e.g., monitoring impairment (T1562), log tampering (T1070), deception evasion (T1036, T1027), and exploitation of trusted relationships (T1199)) ensuring defensive layers are hardened against targeted bypass. At this level, threat assessment becomes a continuous mission-aligned intelligence function that directly informs architecture, monitoring, funding, exercises, and launch readiness decisions across the enterprise.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-5	Mission personnel shall complete annual role-based cybersecurity training prior to being granted access to mission consoles, OT environments, ground systems, or launch infrastructure. Training shall at a minimum include: phishing recognition and reporting (T1566), safe handling of removable media and USB devices (T1204), console hygiene and credential protection (T1078), secure communications practices and protection of mission data, recognition of anomalous telemetry, RF behavior, or OT device responses. Training shall be tailored by functions (examples include): Operators: Secure command execution, command verification procedures, anomaly escalation, Engineers: Secure RF configuration handling, firmware validation, configuration control, Launch crews: OT console integrity, credential discipline during high-tempo operations, Administrators: Privileged access handling, log integrity awareness, monitoring validation. Tabletop scenarios shall demonstrate how common behaviors (e.g., weak passwords, unauthorized USB use, credential reuse, unsafe configuration changes) can degrade mission readiness or impact safety. Completion of required training shall be tracked and verified prior to mission campaign participation. At this level, training reinforces baseline cyber hygiene and role-specific operational security practices that reduce social engineering, user execution abuse, and valid account compromise (T1566, T1204, T1078).	A structured, scenario-based training program shall be delivered using mission simulators, cyber ranges, or digital twins that replicate realistic adversary conditions. Training shall be tailored by functions (examples include): Operators: Secure command execution, command verification procedures, anomaly escalation, Engineers: Secure RF configuration handling, firmware validation, configuration control, Launch crews: OT console integrity, credential discipline during high-tempo operations, Administrators: Privileged access handling, log integrity awareness, monitoring validation. Training shall include hands-on exercises such as: spoofed telemetry dashboards requiring anomaly detection, malicious RF configuration injection attempts, simulated OT/PLC misconfiguration scenarios (T0814), credential harvesting and phishing simulations, baited USB or removable media traps, Insider misuse case studies involving privileged access abuse. Operators shall be evaluated under realistic adversarial pressure conditions, including time-compressed launch scenarios and coordinated cyber-physical anomaly events. Training performance metrics shall be tracked, with certification required for console, OT, and launch system access. Failure to meet training thresholds shall require remediation prior to assignment. Red-team participation shall be incorporated into exercises to validate operator resilience against current threat TTPs, including deception (T1036), monitoring impairment (T1562), and credential abuse (T1078). Training outcomes shall be integrated into HR performance systems, mission readiness reviews, and risk registers to ensure accountability and measurable improvement over time. At this level, end-user training transitions from awareness to operational competency validation under adversarial simulation.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-6	Mission cybersecurity personnel (e.g., SOC analysts, detection engineers, IR responders, security architects) shall receive specialized training on mission systems, ground architectures, OT/ICS environments, and space-specific threat models. Training shall include at a minimum: SPARTA and ATT&CK informed TTP analysis, RF anomaly detection fundamentals and spectrum awareness, OT/ICS risk patterns and unsafe control manipulation (T0814), credential abuse and privilege escalation detection (T1078), log integrity validation and detection of telemetry falsification (T1565), monitoring impairment and alert flooding behaviors (T1562), & forensic log analysis across IT, OT, and mission systems. Defenders shall understand how cyber actions translate into spacecraft risk, launch disruption, loss of command integrity, or safety-of-flight impact and not just host or network level alerts. Organizations shall sponsor relevant industry certifications (e.g., CISSP, GICSP, GCIA, OSCP, GCED) to maintain foundational technical depth. Joint training sessions between defenders, operators, and engineers shall be conducted to improve cross-team understanding of mission workflows and attack impact. Defenders shall participate in quarterly mission exercises to validate detection, response, and escalation readiness under realistic mission conditions. At this level, training ensures defenders can recognize and analyze mission-relevant adversary behaviors rather than generic enterprise IT incidents.	A structured mission-specific defender training pipeline shall be implemented using cyber ranges or digital twins that replicate MOC, ground station, RF, OT/ICS, and launch environments. Defenders shall participate in recurring red/blue/purple team exercises aligned to SPARTA and ATT&CK techniques, practicing against adversary emulation campaigns that include attacks like: telemetry falsification and data manipulation (T1565), monitoring impairment and alert suppression (T1562), credential abuse and account manipulation (T1078, T1098), ICS/PLC exploitation and unsafe state manipulation (T0814), log deletion and anti-forensics (T1070), obfuscation and sandbox evasion (T1027, T1497). Advanced defender skillsets shall include: RF forensic analysis and anomaly triage, STIX-based IOC/IOB creation and deployment, cross-segment correlation (space, link, ground, enterprise), detection engineering for adversary behaviors targeting defensive infrastructure. SOC analysts, detection engineers, and automation developers shall receive training on recognizing deception, alert flooding, poisoned intelligence, and masquerading techniques to prevent operational paralysis. Defender certification in advanced mission-relevant disciplines shall be required and renewed periodically. Readiness metrics shall be documented and reported to mission assurance governance boards. Defender readiness assessments shall be integrated into mission risk registers and launch readiness reviews. At this level, defender training becomes a continuously validated operational capability, directly tied to mission assurance and adversary realism rather than compliance-driven education.

Layer ID	Baseline - Moderate Mission Impact	Enhanced – High Mission Impact
PRE-7	Organizations shall implement structured supplier vetting and component validation processes for all third-party hardware, firmware, software libraries, cloud services, and upstream data sources supporting mission systems, ground infrastructure, launch operations, and defensive tooling. Baseline due diligence shall include at a minimum verification of vendor certifications, completion of security questionnaires, contractual obligations for patching and incident disclosure, and provision of Software Bills of Materials (SBOMs) where applicable. All firmware, drivers, operating system images, and update packages shall require cryptographic signing, and personnel shall validate authenticity prior to installation or deployment. Acceptance testing shall be performed prior to integration into mission environments, including static or dynamic analysis of software components and functional validation of hardware. Firmware hashes shall be verified against trusted baselines before operational use. Organizations shall maintain detailed inventories including component versioning, provenance tracking, and update history for mission-critical systems. Tamper-evident packaging, custody tracking, and authenticity validation shall be enforced for critical mission hardware (e.g., launch systems hardware, PLC racks, cryptographic modules, antenna controllers, networking devices, and mission control infrastructure). These controls reduce the likelihood of embedded compromise associated with supply chain manipulation (T1195), malicious firmware insertion (T0829), unsafe controller modification (T0815), and pre-positioned compromise of COTS devices prior to deployment. At this level, supply chain risk is reduced through vetting, validation, integrity enforcement, and provenance tracking prior to operational deployment. Supply chain risk is systemic and extends beyond direct vendors. These best practices establish preventive baselines but must be complemented by comprehensive Cybersecurity Supply Chain Risk Management (C-SCRM) practices as described in NIST SP 800-161 and related CISA guidance.	Organizations shall implement continuous, "Zero Trust" aligned supply chain validation practices that assume upstream compromise is possible and require ongoing verification of component integrity and authenticity. Vendor SBOMs and software components shall be continuously monitored against threat intelligence feeds and vulnerability disclosures, with findings integrated into SOC workflows and risk registers. Automated integrity validation of firmware and binaries shall occur prior to deployment, and runtime attestation mechanisms (such as secure boot, measured boot, and cryptographic validation of ICS controllers and cryptographic modules) shall be enforced for mission-critical systems where technically feasible. System updates affecting launch sites, mission operations centers, OT controllers, and cryptographic infrastructure shall require dual-party validation and cryptographic verification before execution. Controlled staging environments shall be used to validate updates prior to production deployment. Organizations shall reduce single-vendor dependency for high-impact mission components through architectural resilience measures such as geographically diverse suppliers or redundant sourcing strategies for critical spares. Adversarial validation shall be conducted through supply-chain-focused penetration testing or red-team exercises simulating poisoned firmware, counterfeit components, malicious software libraries, or compromised update channels to validate detection and recovery procedures. Validated supply chain indicators and behaviors shall be shared with partner organizations through structured intelligence-sharing mechanisms to reduce systemic sector risk. Supply chain risk is systemic and extends beyond direct vendors. These best practices establish preventive baselines but must be complemented by comprehensive Cybersecurity Supply Chain Risk Management (C-SCRM) practices as described in NIST SP 800-161 and related CISA guidance. Supply chain controls shall be integrated with runtime monitoring, segmentation, anomaly detection, and mission resiliency measures, recognizing that procurement controls alone cannot eliminate systemic supply chain risk. At this level, supply chain prevention transitions from point-in-time vetting to continuous integrity validation and resilience against embedded compromise.

Appendix C: Ground Segment Functional Decomposition Details

Table 3 provides definitions for each function group, in addition to definitions for the functions within each group.

Table 3 - Ground Segment Functional Decomposition Details

Mission Area	Function group	Function group Definition	Function
Ground Station	Antenna Control & Management	This function group encompasses all hardware and software required to physically orient, calibrate, and manage antennas for reliable spacecraft communication. It includes sensors and actuators for position feedback, servo controllers that translate digital commands into motion, auto-tracking algorithms that maintain pointing accuracy using orbital data, and polarization control to match spacecraft transmission modes. These systems ensure that antennas maintain precise orientation, beam shape, and signal integrity across mission operations.	**Actuators & Sensors:** Devices that sense position or movement and physically enable antenna orientation adjustments
			Servo-driving: Electronic control systems that translate software commands into precise motor actions for antenna movement
			Auto-tracking: Software-based tracking system that continuously adjusts antenna pointing using orbital predictions
			Polarization Handling: Supports linear, circular (RHCP: Right-Hand Circular Polarization, LHCP: Left-Hand Circular Polarization), or mixed polarization to ensure signal integrity and reduce loss due to polarization mismatch.
			Beam Pattern Calibration: Calibrates antenna lobes, beamwidth, and gain to optimize radiation pattern for communication performance.
	Signal Conditioning	Signal conditioning provides the analog front-end for space communications, ensuring that signals captured by antennas are properly transmitted to and from processing systems. This includes coaxial cables and waveguides for signal transport, low-noise amplifiers for boosting weak downlink signals, and high-power amplifiers for ensuring sufficient uplink strength. Frequency conversion hardware shifts signals between bands to ensure compatibility with spacecraft transceivers. Collectively, these components prepare RF signals for reliable demodulation and retransmission.	**Air to Cable (Antenna Interface):** The physical interface capturing the space signal and guiding it into ground RF systems
			Amplification (LNA/HPA): Systems that amplify incoming weak signals or outgoing uplink signals to maintain link quality
			Frequency Conversion: Hardware that shifts RF signals between different frequency bands for compatibility and processing
			Signal Processing & Analog to Digital Conversion (ADC): Hardware that digitizes analog signals and executes real-time signal decoding or analysis
			Data Mux / Demux: Systems that sort and direct command or telemetry streams to appropriate ground processing units
			Ranging / Doppler Measure: Components that assess spacecraft distance and velocity using time and frequency analysis
			Software Defined Radios (SDRs): Reconfigurable radio systems that perform modulation/demodulation in software
	Ground Station Defenses	Ground station defenses mitigate adversarial or environmental RF interference by deploying adaptive technologies. Examples include beam nulling, frequency hopping, and low probability of intercept/exploitation techniques that dynamically adjust how signals are transmitted or received. These capabilities reduce susceptibility to jamming or spoofing, ensuring continuity of spacecraft command and telemetry links even in contested RF environments.	**Anti-jamming Systems:** Technologies that counter RF interference using adaptive signal techniques like nulling or hopping

Mission Operations Center	**Command and Control**	The command and control function group manages the lifecycle of spacecraft commands and telemetry. This includes authoring and sequencing command timelines, providing real-time operator interfaces for anomaly resolution, and maintaining authoritative command and telemetry dictionaries. It also archives command history for auditability and recovery. These systems ensure safe, validated, and accountable interaction between operators and spacecraft subsystems.	**Command Sequencing:** Creates, verifies, and schedules command timelines for delivery to the spacecraft, often coordinating across multiple subsystems
			Payload Command and Control: Interfaces that allow mission operators to configure and control onboard payload systems, such as cameras, sensors, or mission instruments
			Real-time Commanding Interface: Allows operators to issue time-critical commands interactively (e.g., for anomaly resolution or mission replanning). Includes manual input consoles, safety interlocks, and command audit logs.
			Command & Telemetry Dictionary Management: Maintains the authoritative list of valid commands and arguments (the command database) as well as the telemetry database. Critical for parsing, validating, and translating operator intent into spacecraft-understandable formats.
			Command History Logging and Playback: Archives all command activity (uplinked and attempted), allows forensic review, and supports rollback/undo operations. Essential for accountability and recovery.
	Mission Management	Mission management covers planning, scheduling, and orbital prediction functions that align spacecraft activities with mission objectives. It includes software that generates activity timelines, allocates communication resources, predicts orbital passes, and determines precise spacecraft position and velocity. These tools enable mission planners to coordinate limited spacecraft resources, prevent conflicts, and optimize mission outcomes.	**Scheduling:** Allocates and deconflicts ground station contact times, commanding windows, and data downlink sessions. This could be automated via software to identify windows or options for task execution based on constraints and asset availability.
			Planning: Generates mission timelines, activities, and constraints used to guide system operations and ensure successful execution of mission goals.
			Orbit Propagation/Pass Predictions: Calculates when and where the spacecraft will be visible from ground stations, enabling link planning and scheduling. Also contains software algorithms that predict the future position and velocity of a spacecraft based on current state vectors and environmental models
			Orbit Determination: Calculates the spacecraft's precise position and velocity based on distance between the ground antenna and the spacecraft, change in frequency of the signal received from the spacecraft compared to the transmitted frequency, and azimuth and elevation (direction) from the ground station to the spacecraft. Also, it may be used to calculate delta-v and timing of thruster firings to adjust orbit for mission objectives or collision avoidance
	Data Processing	Data processing transforms spacecraft telemetry and payload data into usable mission outputs. It includes telemetry ingestion and decoding, calibration of instrument data into mission products, resource modeling for power, fuel, and bandwidth, and archival of both raw and processed datasets. It also provides data distribution interfaces for partners and external consumers. This group ensures that spacecraft data is validated, preserved, and made available for mission needs.	**Telemetry Ingestion and Decoding:** Ingests spacecraft telemetry data, synchronizes frames, and decodes protocols for use by mission tools and operators.
			Mission Data Processing: Transforms raw instrument data into calibrated, mission-useful outputs through algorithms and processing chains.
			Resource Estimation/Modeling and Allocation: Calculates power, fuel, bandwidth, and data usage to support safe planning and avoid oversubscription of limited spacecraft resources. May overlap or inform Engineering Operations and Rate Checking function.
			Ephemeris Management: Ingests, validates, and propagates spacecraft orbit data used for contact scheduling, pointing, and situational awareness. This can aid with conjunction assessments to predict and evaluate potential collisions with other space objects.

			Telemetry & Mission Data Archival: Stores raw and processed spacecraft data for long-term access, compliance, and reprocessing purposes.
			Data Distribution Services: Publishes mission data to external consumers through APIs, file portals, or data buses for use by mission teams, dashboards, or partner agencies. May also check integrity and correctness of generated data products.
	Engineering Operations	Engineering operations provide analytical and visualization capabilities to monitor spacecraft health and performance. They include real-time dashboards for key telemetry, anomaly detection and rate checking, historical trend analysis, and operator console management. They also manage software updates, time synchronization, and resource modeling. These services enable engineers to diagnose problems, validate performance, and ensure spacecraft safety during operations.	**Spacecraft Performance Monitoring:** Continuously tracks and evaluates key performance indicators from the spacecraft (e.g., power, thermal, attitude control metrics) to ensure nominal behavior.
			Patch and Update Management: Manages software and firmware updates across ground systems and uplink packages for spacecraft software deployments.
			Rate Checkers: Analyze data for sudden or unexpected changes (delta checks) in telemetry, which may indicate anomalies or software/hardware malfunctions. May overlap or inform Data Processing function.
			Anomaly Detection and Trend Analysis: Monitors telemetry and operational patterns to detect faults or unusual behavior, often using rules or machine learning. May overlap or inform Engineering Operations and Rate Checking function.
			Telemetry Trending and Visualization: Enables engineers to visualize historical telemetry data for pattern recognition, degradation tracking, and forecasting.
			Operator Console Management: Manages the mission operator workstation environment, including display layouts, tool configurations, command interfaces, and workstation hardening.
			Time Synchronization Services: Provides trusted time references (e.g., GNSS-sourced PPS signals) to synchronize logs, telemetry frames, command timestamps, and event sequences.
			Asset Resource Modeling: Simulates availability of satellite, ground, and data links. Ensures system-level modeling for feasible plan generation.
			Infrastructure as Code / Platform as Code: Enables reproducible deployment and configuration of ground software and infrastructure components
Launch Integration & Operations	**Launch Integration Testing**	Launch integration testing validates spacecraft and ground segment functionality immediately prior to launch. It includes test harnesses for verifying interfaces, telemetry collection and analysis tools, and procedures for identifying anomalies that could jeopardize mission readiness. These tests occur close to launch operations and ensure that spacecraft systems will perform as expected once integrated with the launch vehicle.	**Test Management:** Controls the necessary logical verification testing as payloads or other components are integrated into the final satellite. This effort is distinct from developer (i.e., contractor) satellite manufacturing and integration prior to major transport to the launch center. This is defined due to the proximity of the efforts to operations and the ability to immediately impact mission capability after launch.
			Data Analysis: Collection and analysis of integration testing data while final integration occurs prior to launch. This effort is distinct from developer (i.e., contractor) satellite manufacturing and integration prior to major transport to the launch center. This is defined due to the proximity of the efforts to operations and the ability to immediately impact mission capability after launch.

	Spacecraft Communication	This group provides direct spacecraft communication during launch and integration activities, using umbilical cables or local RF links. It allows operators to command the spacecraft, configure states, and receive telemetry while the spacecraft is in the launch vehicle fairing. These links ensure the spacecraft can be safely managed prior to separation and orbit insertion.	**Telemetry and Commanding Relay:** Data communication with the satellite supported over umbilical cable or through local radio frequency communication within the launch vehicle faring. This communication is necessary to command states of the satellite prior to and during launch. This communication also receives satellite state information via telemetry. The communication is relayed between other facilities such as the launch center or the mission operations center.
	Launch Control Center	The launch control center provides the command sequencing, abort logic, and uplink software used to control the launch vehicle. It includes operator interfaces for manual overrides and automated safety interlocks. These systems ensure that launch operations can be executed safely and that aborts can be initiated if unsafe conditions are detected.	**Launch Control Software:** Manages the launch vehicle commanding process, including command sequencing, uplink, and manual or automated launch abort capabilities.
	Launch Monitoring Systems	Launch monitoring systems collect and visualize telemetry from the launch vehicle in real time. They include health monitoring algorithms, data acquisition processors, and graphical displays for decision-makers. Their primary role is to ensure launch safety by detecting anomalies early and enabling rapid abort decisions if required.	**Flight System Safety:** Launch safety, and automated/manual launch abort if unsafe conditions are detected. **Telemetry Collection:** Acquires, processes, and archives launch vehicle telemetry and tracking in real time for performance tracking and safety assurance. **Launch Visualization:** Provides overall visualization of launch telemetry and information to support real-time decision-making during launch.
	Facility Management	Facility management covers industrial control and operational technology systems that enable physical launch infrastructure. These include SCADA/PLC systems for power, fuel handling, HVAC, and water systems. Secure operation of these systems is essential to ensure that the launch site is safe, reliable, and resilient to both cyber and physical disruptions.	**Industrial Control Systems (ICS) / Operational Technology (OT):** Control of physical systems supporting launch. ICS includes technology such as supervisory control and data acquisition (SCADA), programmable logic controllers (PLCs). OT includes monitor and control of the broader physical operations and infrastructure
Ground Networking Services	**Network Access Control Services**	Network access control services secure the flow of data within ground mission networks. They include firewalls, VPNs, routing policies, and protocol stack implementations tailored to mission protocols (e.g., CCSDS). They also provide encryption at the network and transport layer. This ensures that mission data is protected from interception or manipulation while traversing internal and external networks.	**Perimeter Enforcement:** Manages ingress/egress points into the ground network via firewalls, VPN concentrators, and network zoning enforcement mechanisms. **Transport/Network-Layer Encryption:** Encrypts network-layer traffic across untrusted or external links, preserving confidentiality and integrity of command, telemetry, and mission data. **Routing and Switching Operations:** Core routing and switching infrastructure that supports data flow between mission components and external interfaces. **Protocol Stack Management:** Implements mission-specific transport and application protocols (e.g., CCSDS TM or AOS for telemetry, TC command, and CFDP for file transfers). **Routing and Traffic Integrity:** BGP Hardening, Route Integrity, and Traffic Shaping

	Network Monitoring and Visibility	This group provides visibility into mission networks by monitoring traffic for anomalies, intrusions, or policy violations. Using IDS/IPS, log collectors, and SIEM platforms, it ensures that adversary activities are detected quickly and that network operators maintain situational awareness of mission communications.	**Network Traffic Monitoring:** Monitors ground network traffic and infrastructure for indications of compromise or other network policy violations. Supports alerting and forensic analysis. Network monitoring (e.g., NOCs) is sometimes different than host or mission monitoring.
	External Connectivity Services	External connectivity services govern secure data exchange with partners and enterprise IT systems. This includes firewalls and DMZ gateways for inter-agency or commercial collaboration, as well as secure enterprise integration for services like email or file sharing. These functions enforce policy boundaries while enabling necessary mission collaboration.	**Mission Partner Integration:** Manages network connectivity and policy enforcement for communications with international and inter-agency mission partners. Depending on the mission, partners may have commanding / configuration capability for payloads.
	External Connectivity Services		**Enterprise IT Integration:** Provides access from the ground network to enterprise IT services (e.g., email, file shares, software repositories).
	Network Time Services	Network time services provide synchronized and trusted time across mission networks, derived from GNSS or master clocks. Using NTP or PTP, these services ensure that command timestamps, telemetry packets, and event logs remain aligned. Accurate timing is essential for mission coordination, orbit prediction, and forensic analysis.	**Time Distribution Management:** Distributes trusted time references across networked systems using protocols like NTP or PTP, sourced from GNSS or dedicated time servers.
	Network Storage Services	This group provides centralized mission storage (e.g., NAS/SAN systems) for telemetry, logs, mission data, and backups. It supports redundancy, indexing, and long-term archival, ensuring that mission data is both accessible and protected from loss.	**Mission Storage Services (e.g., NAS/SAN):** Provides centralized storage for telemetry, logs, images, and other mission data, accessible over the ground network.
	Management Network	The management network provides secure out-of-band or bootstrap access for mission systems. It supports console servers, IP-based KVMs, and remote provisioning tools, enabling operators to maintain system control during incidents, perform recovery, or initialize systems without relying on operational paths.	**Out-of-Band Access Control:** Provides isolated access to network and system management interfaces (e.g., serial consoles, power management) to maintain control during incidents. This could be remote management / interconnect vice OOB.
			Bootstrapping Protocols: TFTP/FTP Management for System Bootstrapping
	IP Address & Name Services	This group manages addressing and naming within mission networks. DHCP, DNS, and IPAM systems provide consistent assignment of IP addresses and resolution of system names. These services are foundational for mission system connectivity and secure communication.	**IPs and DNS: DNS / IP Address Management:** Assigns and resolves IP addresses and domain names for mission systems.
Ground Security Operations Center	**Mission Monitoring and Situational Awareness**	Mission monitoring and situational awareness aggregates spacecraft telemetry, ground system health, and cyber indicators into a fused operational picture. This enables operators to detect anomalies, track threats, and make informed decisions based on both mission and cybersecurity data.	**Asset and Threat Telemetry Aggregation:** Aggregates mission and cybersecurity telemetry to maintain awareness of critical assets and detect signs of compromise or misconfiguration.

	Defensive Cyber Ops (DCO)	DCO services actively defend mission systems by detecting, correlating, and responding to adversary tactics. They include intrusion detection, anomaly detection, threat intelligence correlation, and automated defense actions. This ensures that adversarial activity is identified and contained before it threatens mission objectives.	**Intrusion Detection / Anomaly Detection:** Detects adversarial activity or anomalous behavior using signature-based and behavior-based analysis techniques across the ground segment.
	Mission Monitoring and Situational Awareness	Mission monitoring and situational awareness aggregates spacecraft telemetry, ground system health, and cyber indicators into a fused operational picture. This enables operators to detect anomalies, track threats, and make informed decisions based on both mission and cybersecurity data.	**Vulnerability Risk Management:** Tracks, assesses, and prioritizes vulnerabilities within mission and enterprise ground systems; coordinates patching and mitigation strategies.
	Incident Response & Management	Incident response and management coordinate the detection, triage, containment, and recovery of cybersecurity incidents. It includes case management systems, forensic analysis tools, and malware reverse engineering capabilities. This group ensures that missions can recover from cyber events while minimizing impact.	**Malware and Artifact Analysis:** Collects memory images, binary artifacts, logs, and telemetry anomalies for reverse engineering, root cause identification, and malware attribution.
			Cyber Incident Coordination: Coordinates detection, triage, escalation, response, and reporting of cybersecurity incidents across the mission enterprise.
	Defensive Cyber Ops (DCO)	DCO services actively defend mission systems by detecting, correlating, and responding to adversary tactics. They include intrusion detection, anomaly detection, threat intelligence correlation, and automated defense actions. This ensures that adversarial activity is identified and contained before it threatens mission objectives.	**Active Defense Execution:** Conducts active defense operations, such as threat hunting, cyber deception, and tactical containment to defend the ground segment.
			Threat Intelligence Correlation: Correlates incoming threat intelligence (IOCs, IOBs, STIX patterns, TTPs) from external sources and internal sensors with mission telemetry, logs, and anomalies.
			SOC Automation & Orchestration (SOAR): Implements automated playbooks for detection, response, and alert triage to accelerate mitigation of ground cyber threats.
	Deception and Decoy Services	Deception services deploy honeypots, canaries, and decoy data to lure and detect adversaries. These tools help reveal attacker techniques, delay their progress, and provide defenders with early warning of intrusion attempts within the mission network.	**Adversary Deception Techniques:** Deploys and monitors honeypots, and canaries to lure attackers and detect lateral movement or tool usage.
	Mission Monitoring and Situational Awareness	Mission monitoring and situational awareness aggregates spacecraft telemetry, ground system health, and cyber indicators into a fused operational picture. This enables operators to detect anomalies, track threats, and make informed decisions based on both mission and cybersecurity data.	**Red Team Integration & Adversary Emulation:** Supports recurring Purple Team events using adversary emulation to test SOC readiness. Realistic payloads mimic threats using synthetic telemetry/malware.
	Launch Security Services	This group provides logical and cryptographic protections specific to launch operations. It ensures that telemetry and commanding are encrypted, that access to the	**Cryptographic Services:** Provides encryption and decryption of commanding and telemetry for the launch operations center
			Access Control: Logical access control to launch control center and launch site

		launch control center is restricted to authorized users, and that cyber defense monitoring is active during the critical launch window. These services protect launch operations from malicious disruption.	**Cybersecurity Operations:** Defensive monitoring of launch operations center information systems and perform response and recovery for cyber incidents.
	MOC Security Services	Mission Operations Center (MOC) security services provide core cyber protections for mission-critical ground infrastructure. They include cryptographic services for safeguarding command and telemetry data, access control for operators and administrators, host and log monitoring for anomaly detection, patch and configuration management, and secure remote access services. Together, these functions enable the MOC to enforce strong security hygiene and ensure mission assurance against cyber threats.	**Crypto Services:** Services that manage encryption keys and cryptographic modules used to protect command, control, and telemetry data
			Cyber Access Control: Services that manage user accounts, passwords, and authorization policies to control operator and system-level access
			Host Monitoring: Capabilities that detect and report on abnormal system behavior, process execution, file integrity, and user activity across mission-critical ground servers
			Patch and Vulnerability Management: Capabilities that identify, prioritize, and remediate known security flaws in mission-critical systems and applications
			Secure Configuration Management: Ensures that mission systems operate using hardened configurations, detect deviations, and automatically correct unauthorized changes
			Audit Logging & Centralized Log Management: Enables collection, correlation, and storage of system and application logs for detection and investigation. MOC security monitoring often different than enterprise-wide monitoring or ground station specific monitoring.
			Remote Access Security & Session Management: Manages and secures all pathways into the Mission Operations Center, especially for remote users and administrators
Ground Station as a Service (GaaS)	**Access & Credential Management**	Access and credential management govern the lifecycle of mission identities, API keys, and authentication tokens. It ensures secure issuance, storage, rotation, and revocation of credentials, protecting systems from unauthorized access and privilege misuse.	**API Credential and Token Management:** Maintains security tokens, API keys, and user credentials for interfacing with GaaS provider systems; includes rotation and revocation capabilities.
	Access Scheduling Interface	This function group provides APIs and interfaces for scheduling spacecraft uplink and downlink sessions. It ensures that authenticated operators can request communication windows while enforcing contact priorities and resource constraints.	**Scheduling API Access:** Interface that enables mission operators to schedule uplink/downlink contacts using vendor-exposed APIs or GUIs, typically authenticated with tokens or API keys.
	Command and Telemetry Gateways	These gateways authenticate and process spacecraft commands for uplink and distribute downlinked telemetry to consumers. They enforce policy boundaries between customer systems and vendor ground infrastructure, ensuring secure and accountable data flows.	**Command Uplink Gateway:** Processes spacecraft commands submitted to the GaaS provider, authenticates payload, and queues for uplink over vendor-controlled RF chain.
			Telemetry Downlink Gateway: Provides access to spacecraft telemetry data post-pass-through secure API, file portal, or storage buckets.
	Encryption & Network Security	This group ensures confidentiality and integrity for all spacecraft command, telemetry, and mission data transmissions. It implements FIPS 140-2 or NSA Type-1 encryption across shared or untrusted networks, protecting sensitive information and preventing adversary exploitation.	**GaaS Link Encryption:** Encrypts all TT&C and mission data transmissions via FIPS 140-2 or NSA Type-1 approved encryption to ensure confidentiality and integrity across shared infrastructure.

	Service Subscription Management	In government-as-a-service (GaaS) models, this group manages customer subscription tiers, usage tracking, and billing. It enforces prioritization of spacecraft contact scheduling and resource allocation according to contractual agreements.	**GaaS Subscription Tiers:** Enables customer selection between pay-as-you-go and unlimited use tiers, influencing contact priority, resource availability, and billing models.

Appendix D: Attack and Defense Analysis of Viasat KA-SAT Event

D-1. Introduction

In February 2022 there was a cyber attack on the Viasat KA-SAT ground segment managing their satellite communication (SATCOM) services across the broader Europe region. The cyber operations were later attributed by the United States Department of State[1], the Council of the EU[2], and the United Kingdom Government[3] to Russian cyber actors with the intent to affect SATCOM mission capabilities in correlation with Russian Invasion of Ukraine. This significantly publicized and examined event provides specific context and purpose for how a ground segment can be attacked through cyber actions.

We provide an analysis of Viasat events as reported by Mark Colaluca and Nick Saunders from Viasat's Government Group at DEF CON 31 under the talk "Defending KA-SAT"[4]. The attack impacts were described in relation to "wiper malware" deployed to ~50,000 SATCOM modems and Dynamic Host Configuration Protocol (DHCP) manipulation attacks that interrupted network capabilities. These combined attacks caused significant disruptions to Viasat's SATCOM services through physical modems being disabled and overall network disruptions that effectively denied targeted users' mission capabilities.

While Viasat described aspects of the attack through their observations and response, the explanations were not normalized to any nomenclature or framework for attack and defense of a ground segment. We present how this report's MITRE ATT&CK techniques and DiD countermeasures explain the attack methods used and defenses that would have been able to stop the cyber actor's attack chain. This analysis helps to explain and bolster the value of this framework and DiD countermeasures to protect a ground segment.

It should be noted that we do not specifically know what ground segment defenses were in place before the KA-SAT attack occurred. However, through deduction we can assume that all of the identified ATT&CK techniques identified as being successful would have either bypassed the identified framework countermeasures or those countermeasures were not present.

[1] https://2021-2025.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/
[2] https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
[3] https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion
[4] https://www.youtube.com/watch?v=qI_ICtX3Gm8

D-1.1. Attacks Against Functional Decomposition

We leverage the Ground Segment Mission Functional Breakdown previously shown in Figure 4 to depict where the attacks occurred in Figure 5. The focus of the attacks occurred within the Ground Networking Services mission area. More specifically to the functional groups Network Access Control Services, External Connectivity Services, Management Network, and IP Address & Name Services that were attacked. We describe how each functional group and functions were attacked with associated ATT&CK techniques.

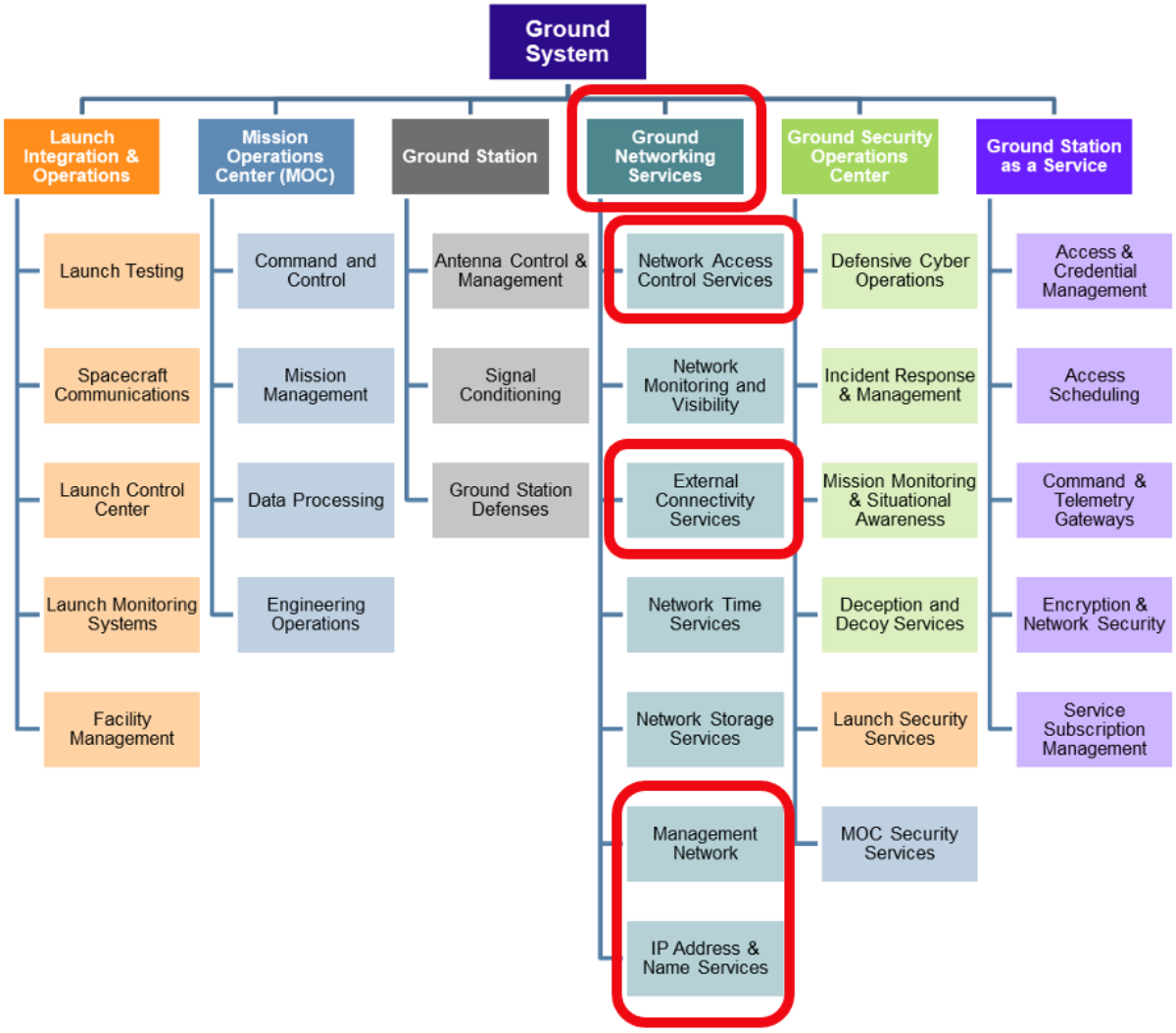

Figure 5 - Ground Segment Functions Attacked During Viasat KA-SAT Event

Based on the information provided by Viasat, we can depict the primary attack techniques used against the Viasat ground segment. The initial intrusion occurred through Network Access Control Services at the perimeter enforcement boundary. Compromised VPN credentials were used to authenticate into a trusted ingress point, representing a compromise of remote access governance and network segmentation. This aligns with technique **T1078: Valid Accounts**, which were stolen credentials that provided legitimate

access to the management plane, and **T1133: External Remote Services**, that reflects an abuse of VPN pathways into mission infrastructure. Because the VPN termination point provided connectivity into management infrastructure without sufficiently strict segmentation, this also reflects elements of **T1199: Trusted Relationship**, where enterprise or externally accessible services were implicitly trusted and allowed pivoting into sensitive mission systems.

Once inside the trusted boundary, the adversary moved across the Management Network. According to the Viasat explanation, the attackers pivoted to management servers, staged tooling, and leveraged legitimate software distribution mechanisms to deploy a malware binary to modems. This was not a novel and sophisticated attack method utilizing Lateral Movement techniques; this attack simply abused the authenticated management-plane. The destructive wiper payload overwrote both primary and fallback flash filesystems to permanently disable modems. This attack accomplished a unique combination of Persistence through **T1542.003: Pre-OS Boot** and Impact with the wiper capability through **T1565.001: Data Manipulation: Stored Data Manipulation.** The end mission impact was tens of thousands of modems rendered unusable, and this reflects aspects of **T1499: Endpoint Denial of Service**.

In addition to the wiper attack, there was parallel DHCP attack that originated from within Network Access Control Services and IP Address & Name Services. In this phase, authenticated end-user terminals were used to craft malicious DHCP interactions to confuse control logic. While the Viasat explanation did not describe how the attacker achieved terminal authentication, the attacker's Initial Access was effectively **T1199: Trusted Relationship**. The terminal communication was manipulated through **T1565.001: Data Manipulation: Stored Data Manipulation** through malicious capabilities on the terminal that enabled DHCP manipulation. **T1565.003: Data Manipulation: Runtime Data Manipulation** for network traffic was then accomplished through abusing DHCP message handling to alter the DHCP runtime control-plane state. This attack also reflects a form of denial of service consistent with **T1498: Network Denial of Service** but not in a volume/flooding sense, rather by destabilizing network services through protocol abuse.

These ATT&CK techniques can be aligned into an attack chain as shown in

Table 4 - Defined Attack Chains Against Viasat Ground Segment

	ATT&CK Tactic	ATT&CK Technique	
Wiper Attack	Initial Access	T1078	Valid Accounts
		T1133	External Remote Services
		T1199	Trusted Relationship
	Persistence	T1542.003	Pre-OS Boot
	Impact	T1565.001	Data Manipulation: Stored Data Manipulation
		T1499	Endpoint Denial of Service
DHCP Attack	Initial Access	T1199	Trusted Relationship
		T1565.001	Data Manipulation: Stored Data Manipulation
	Impact	T1565.003	Data Manipulation: Runtime Data Manipulation
		T1498	Network Denial of Service

D-1.2. DiD and Functional Group Defense

The DiD framework developed in this report enables the identified functional groups and ATT&CK techniques to be matched through Attachment 1 with applicable DiD sublayer countermeasures in Appendix B. This knowledge set enables analysis of how a properly architected and enforced set of ground segment countermeasures could have disrupted or prevented key stages of the Viasat attack chain. Rather than relying on isolated recommended countermeasures, this approach provides coordinated DiD protections across the affected functional groups. When implemented collectively, these DiD countermeasures would directly constrain adversary entry points, limit movement, protect critical management interfaces, and increase visibility into anomalous activity that could have ultimately broken the progression of the Viasat attack scenario before it could result in widespread impact. This is the purpose and value of how the DiD framework utilizes multiple sublayers of countermeasures to support resilient defense.

We first start with utilizing the Viasat identified ATT&CK techniques that are associated with each of the functional groups in the Ground Networking Services mission area: Network Access Control Services (NACS), External Connectivity Services (ECS), Management Network (MN), and IP Address & Name Services (IANS). Each functional group already has likely ATT&CK techniques identified in Attachment 1, and we correlate these techniques with the functional group techniques. In Table 5 we identify how each functional group's techniques align with DiD sublayer countermeasures from Attachment 1 through darkened cells indicating a technique match. This matching now provides a direct link between the attack chain and recommended DiD sublayer countermeasures.

Table 5 - Viasat Attack Identified DiD Sublayer Countermeasures

		NACS	ECS	MN	IANS
DAT-1	Encryption	■	■	■	■
DAT-2	Data Loss Prevention - Data	■	■		
DAT-3	Access Control - Data		■	■	■
DAT-4	Sensitive Data Access Control		■	■	
CSW-6	Supply Chain Risk Management - Software	■		■	
END-2	Logging & Auditing		■	■	■
END-3	Authentication - Endpoint	■	■		
END-6	Configuration Control / Endpoint Baseline	■		■	■
END-7	Separation of Duties	■	■	■	
END-9	File Integrity	■		■	■
END-10	Host Firewall	■			
END-14	Patch Management	■	■		■
END-15	File Permissions	■		■	■
END-16	Remote Access	■	■	■	
END-17	Service Configuration				■
END-18	User Least Privilege		■		
END-19	Vulnerability Scanning	■	■		
NET-1	Reverse Proxy	■			
NET-2	Access Control Lists	■	■	■	■
NET-3	Authentication – Network Administration	■	■	■	■
NET-4	Configuration Management - Network	■	■	■	■
NET-5	Hardening – Network Devices	■		■	■
NET-6	Diversification of Network Paths	■			
NET-7	Documentation/Diagrams - Network	■	■		
NET-8	Internal Firewall	■	■	■	
NET-9	Logging - Network	■	■	■	■
NET-10	Network Access Control - Device Authorization	■	■	■	■
NET-11	Network Operations Center	■			
NET-12	Network Time Protocol	■			
NET-13	Port Security	■		■	
NET-14	Segmentation	■	■	■	■
NET-15	Simple Network Management Protocol	■			
NET-16	Trunking	■			
NET-17	Remote Management Access	■	■	■	
NET-18	Web Proxy	■	■		
NET-19	Wireless	■			
CND-2	Hunting				■
CND-3	Threat Intelligence		■		■
CND-4	Intrusion Detection and Prevention Systems	■	■	■	■
CND-6	Security Sensors	■		■	
CND-7	Security Information & Event Manager	■	■	■	
CND-8	Security Operations Center		■		
CND-9	Test Access Points	■		■	
PER-1	Web Application Firewall		■		
PER-2	Virtual Private Network / Remote Access	■	■	■	
PER-3	Data Loss Prevention – Perimeter		■		
PER-4	Demilitarized Zones / Security Zones	■	■	■	
PER-5	Perimeter Firewall	■	■	■	■

		NACS	ECS	MN	IANS
PHY-1	Badging / Doors	■		■	
PHY-2	Fire Suppression	■			
PHY-3	Gates/Guards	■		■	
PHY-4	Logging - Physical	■		■	
PHY-5	Mission Security Personnel			■	
PHY-6	Infrastructure Diversity				■
PRE-1	Personnel Awareness		■	■	
PRE-2	Personnel Management		■	■	
PRE-3	Security Assessments	■	■	■	■
PRE-4	Threat Assessment	■	■	■	■
PRE-5	End-user Training		■	■	
PRE-6	Information Security Staff Training		■	■	
PRE-7	Supply Chain - Prevention	■		■	

Each DiD sublayer countermeasure is defined in Appendix B and this countermeasure set provides holistic aspects to consider for DiD capabilities across the functional groups. While Table 5 provides all the technique-related countermeasures across a system, there is a specific set of countermeasures that could have effectively stopped this specific Viasat attack chains as described in Table 4. In the following sub-sections, we leverage the technique mappings to DiD countermeasures in Attachment 1, like was accomplished for Table 5, but we also perform system security engineering to select the specific countermeasures statements that could have broken the attack chain at each step. These statements are drawn directly from Appendix B with minimal modification. While tailoring of countermeasures is encouraged, we maintained the original language in this demonstration to clearly illustrate how Appendix B can be applied. Each attack chain breakage is described through a capability-grouping of specific DiD countermeasure statements from Appendix B that correspond to the techniques identified in Table 4. This analysis is helpful for attack remediation and preventing future attacks of this nature.

D-1.2.1. Wiper Attack Countermeasures

T1078: Valid Accounts | Authentication and Identity Control Capability

- [NET-3] Multi-factor authentication (MFA) shall be required for all IT operator and administrative accounts that manage network infrastructure, including routers, switches, firewalls, VPN concentrators, console servers, DNS/DHCP/IPAM platforms, crypto appliances, and federation gateways.
- [NET-3] Shared vendor or default administrative accounts on network and OT-connected devices shall be replaced with named accounts tied to individual identities.
- [NET-3] Separate identities shall be maintained for IT network administration and OT/mission network operations to prevent convergence of privileges across environments.

- [END-3] Strong authentication controls shall be enforced for all IT operator, administrative, engineering, and mission-impacting accounts accessing ground segment endpoints.
- [END-3] Service accounts shall be segregated from user identities, assigned least-privilege permissions.
- [PRE-2] All operator, administrator, engineer, contractor, and vendor accounts associated with Mission Operations Centers (MOC), launch control environments, ground station equipment, OT PLCs, cryptographic systems, and security infrastructure shall be reviewed at least quarterly to eliminate stale, orphaned, or unnecessary accounts.

T1133: External Remote Services | Remote Access and External Connectivity Control Capability

- [PER-2] Device posture validation shall be enforced prior to granting access, including verification of patch level, endpoint protection status, and configuration compliance.
- [PER-2] VPN concentrators shall be deployed within controlled DMZ environments logically separated from OT networks, launch control systems, and mission-critical enclaves.
- [PER-4] Externally reachable services, including web portals, identity and access management systems, VPN concentrators, APIs, file transfer services, and partner connectivity nodes, shall be deployed within dedicated Demilitarized Zones (DMZs). These DMZs shall be logically and physically separated from core mission networks (e.g., areas that include sequencing systems, command uplink interfaces, telemetry ingestion platforms, storage systems, and OT control environments).
- [NET-3] Where native MFA is not supported on infrastructure devices, administrative access shall be restricted through hardened jump hosts that enforce MFA prior to session establishment.
- [END-3] Certificate-based or hardware-token-backed authentication shall be required for OT engineering accounts, mission administrators, launch control personnel, network infrastructure administrators, cryptographic key custodians, GaaS control-plane operators, and security platform administrators.
- [END-16] In limited areas where remote connectivity is mission-essential for operational continuity, maintenance, anomaly response, or vendor support, remote access shall be tightly controlled, explicitly authorized, and not continuously available by default. Remote connectivity shall be enabled only when operationally required and disabled when not actively in use.

- [END-16] All remote sessions shall be logged, including authentication events, commands executed, configuration changes, and file access activity. Session activity shall be monitored and forwarded to centralized logging and security monitoring systems to enable investigation of credential misuse, remote service exploitation, or command abuse.

T1199: Trusted Relationship | Segmentation and Network Boundary Enforcement Capability

- [PER-5] Next-Generation Firewalls (NGFWs) shall be deployed at all mission ingress and egress boundaries, including connections to partner networks, enterprise IT, internet-facing services, and external RF or gateway environments. Firewalls shall enforce strict IP, port, and protocol allow-listing, permitting only explicitly documented and mission-approved traffic flows (e.g., CCSDS links, approved partner VPN tunnels, telemetry distribution paths).
- [NET-2] Access Control Lists (ACLs) shall enforce a default-deny posture at all logical network boundaries within the ground architecture, including between enterprise IT, mission IT, OT networks, launch environments, partner enclaves, and externally facing services. Only explicitly authorized protocols, ports, hosts, and services required for mission operations (e.g., telemetry transport, command pathways, approved ICS protocols such as Modbus/TCP where applicable) shall be permitted.
- [NET-8] Internal firewalls shall be deployed between mission enclaves to enforce explicit trust boundaries and least-privilege connectivity using a default-deny model.
- [NET-14] The network shall implement VLANs, internal firewalls, and routed boundaries to separate operator consoles, C2 workstations, antenna controllers, OT PLCs, fueling systems, mission management systems, and enterprise IT.
- [NET-14] Default-deny communication policies shall be enforced between segments, allowing only explicitly authorized mission-required traffic (e.g., uplink command paths, telemetry ingest flows, safety monitoring feeds).
- [NET-14] Prevent direct partner or enterprise access to mission-critical enclaves. Isolate ingestion, processing, analytics, archives, and distribution tiers to limit data manipulation and pivot opportunities.

T1199: Trusted Relationship | Device & Network Access Control Capability

- [NET-3] Device authorization controls shall ensure that only approved administrative workstations may connect to network enforcement devices or management planes.
- [NET-3] Unmanaged or rogue endpoints shall be prevented from accessing management interfaces.

- [NET-10] Network Access Control (NAC) shall be deployed across all wired and wireless access points supporting mission networks to enforce device validation prior to granting network access. All consoles, engineering laptops, operator workstations, and administrative systems shall undergo posture validation before joining mission VLANs or management enclaves. Validation checks shall include patch status, anti-virus/EDR presence, configuration compliance, and domain enrollment where applicable.

T1565.001: Data Manipulation: Stored Data Manipulation & T1542: Pre-OS Boot & T1499 Endpoint Denial of Service | Configuration Control & Hardening Capability

- [NET-4] Golden configuration baselines shall be established and maintained for each network device role, including routers, switches, firewalls, VPN concentrators, DNS/DHCP/IPAM platforms, console servers, crypto appliances, monitoring taps, and partner connectivity gateways.
- [NET-4] All configuration changes shall require documented review and approval prior to deployment.
- [NET-4] Insecure or legacy protocols and daemons shall be disabled by policy and verified through automated checks.
- [NET-5] Network devices supporting mission operations, launch infrastructure, and OT control networks shall be hardened using industry-recognized benchmarks such as CIS or DISA STIG guidance.
    - E.g., Secure boot and boot-time verification mechanisms ensure that management plane systems, including network infrastructure and remote administration endpoints, only execute trusted and validated firmware and software, preventing adversary persistence or destructive modification of critical systems.
- [NET-5] SNMPv3 with authentication and encryption shall be required for network monitoring and management functions. Default accounts, shared credentials, and vendor-provided credentials shall be removed or disabled, and unique named administrative accounts shall be enforced where supported.

D-1.2.2. DHCP Attack Countermeasures

T1199: Trusted Relationship & T1565.001: Data Manipulation: Stored Data Manipulation | Terminal Integrity Monitoring Capability

- [END-9] File Integrity Monitoring (FIM) shall be deployed on mission-critical endpoints and directories to detect unauthorized modification of sensitive files,

firmware images, and configuration artifacts across ground station systems, mission operations infrastructure, launch environments, networking services (e.g., DNS/DHCP), and security platforms.

T1565.003: Data Manipulation: Runtime Data & T1498: Network Denial of Service | DNS / DHCP / IPAM Security Controls Capability

- [NET-2] Network configuration enforcement shall be cryptographically controlled, continuously validated, and tightly integrated with mission assurance workflows. Configurations shall require cryptographic integrity protection and attestation prior to deployment, ensuring that routing and enforcement policies cannot be silently altered.
- [NET-3] Certificate-based or hardware-token-backed authentication shall be required for all privileged access to routers, switches, firewalls, VPN concentrators, DNS/DHCP/IPAM systems, console servers, crypto appliances, and identity components.
- [NET-3] Authentication telemetry from all network management planes shall stream into SOC monitoring systems for correlation with ACL changes, configuration drift, file integrity alerts, and physical telemetry events. Automated analytics shall detect anomalous administrative behavior such as off-hours access, rapid configuration changes, geographically inconsistent logins, or privilege escalation attempts.
- [NET-5] Network-layer protections such as DHCP snooping, dynamic ARP inspection, and rate limiting shall be enabled where feasible to reduce exposure to denial and man-in-the-middle staging attempts.

D-1.2.3. Enabling Countermeasure Capability

For both the wiper and DHCP attacks, breaking the attack chain techniques would be equally enabled through a logging, monitoring, and detection capability implemented across the ground segment function. This capability is enabled through the Ground Security Operations Center mission area and associated functional groups.

All Attack Chain Techniques | Logging, Monitoring, and Detection Capability

- [CND-4] Intrusion Detection and Prevention Systems (IDS/IPS) shall be deployed at mission-critical network choke points, including command uplink gateways, telemetry ingestion interfaces, planning enclave boundaries, VPN termination points, DNS/DHCP infrastructure, and other externally exposed or high-value segments. These systems shall at a minimum be configured to detect exploitation attempts

against portals and remote services, adversary-in-the-middle activity, anomalous VPN or SSH behavior, and denial-of-service precursors.

- [NET-3] Automated analytics shall detect anomalous administrative behavior such as off-hours access, rapid configuration changes, geographically inconsistent logins, or privilege escalation attempts. IDS/IPS shall detect anomalous VPN/SSH behavior, remote service exploitation, and denial-of-service precursors.
- [NET-9] Detailed logging shall be enabled on all routers, switches, firewalls, VPN concentrators, crypto gateways, and other network infrastructure supporting mission operations.
- [NET-9] Logging shall capture ACL hits and denials, control-plane events, routing changes, failed authentication attempts, configuration modifications, VPN session activity, crypto negotiation failures, and abnormal protocol usage. (NET-9)
- [NET-9] Logs shall be forwarded to a centralized SIEM or SOC monitoring platform to prevent local tampering and to enable correlation with endpoint, application, and mission telemetry events.

Appendix E: Acronym List

Acronym	Definition
ABAC	Attribute-Based Access Control
ACL	Access Control List
ACU	Antenna Control Unit
ADC	Analog to Digital Conversion
ASLR	Address Space Layout Randomization
C2	Command and Control
CCSDS	Consultative Committee for Space Data Systems
CFDP	CCSDS File Delivery Protocol
CFG	Control Flow Guard
CI/CD	Continuous Integration / Continuous Deployment
CIS	Center for Internet Security
CNSS	Committee on National Security Systems
COOP	Continuity of Operations
COTS	Commercial Off-The-Shelf
CVE	Common Vulnerabilities and Exposures
CWE	Common Weakness Enumeration
DCO	Defensive Cyber Operations
DEP	Data Execution Prevention
DHCP	Dynamic Host Configuration Protocol
DiD	Defense-in-Depth
DISA	Defense Information Systems Agency

DLP	Data Loss Prevention
DMZ	Demilitarized Zone
DNS	Domain Name System
DoS	Denial of Service
DPI	Deep Packet Inspection
DSP	Digital Signal Processing
DTP	Dynamic Trunking Protocol
EAP-TLS	Extensible Authentication Protocol - Transport Layer Security
EDR	Endpoint Detection and Response
FFRDC	Federally Funded Research and Development Center
FIM	File Integrity Monitoring
FIPS	Federal Information Processing Standards
FTP	File Transfer Protocol
GaaS	Ground Station as a Service
GNSS	Global Navigation Satellite System
GSE	Ground Support Equipment
GUI	Graphical User Interface
HIDS	Host-based Intrusion Detection System
HIPS	Host-based Intrusion Prevention System
HMI	Human Machine Interface
HPA	High-Power Amplifier
HSM	Hardware Security Module
HSTS	HTTP Strict Transport Security

HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVAC	Heating, Ventilation, and Air Conditioning
IAM	Identity and Access Management
ICMP	Internet Control Message Protocol
ICS	Industrial Control Systems
IDS	Intrusion Detection System
IDPS	Intrusion Detection and Prevention System
IKE	Internet Key Exchange
IOB	Indicator of Behavior
IOC	Indicator of Compromise
IP	Internet Protocol
IPAM	IP Address Management
IPS	Intrusion Prevention System
IPSec	Internet Protocol Security
IR	Incident Response
ITAR	International Traffic in Arms Regulations
IT	Information Technology
JIT	Just-in-Time
kCFI	Kernel Control Flow Integrity
KVM	Keyboard, Video, Mouse
LDAP	Lightweight Directory Access Protocol
LHCP	Left-Hand Circular Polarization

LNA	Low-Noise Amplifier
LSASS	Local Security Authority Subsystem Service
MAC	Media Access Control / Mandatory Access Control
MACsec	Media Access Control Security
MFA	Multi-Factor Authentication
MIB	Management Information Base
MITM	Man-in-the-Middle
MOC	Mission Operations Center
MSA	Managed Service Account
mTLS	Mutual Transport Layer Security
NAC	Network Access Control
NAS	Network Attached Storage
NGFW	Next-Generation Firewall
NIST	National Institute of Standards and Technology
NOC	Network Operations Center
NTP	Network Time Protocol
NTS	Network Time Security
OOB	Out-of-Band
OT	Operational Technology
OWASP	Open Web Application Security Project
PAM	Privileged Access Management
PAW	Privileged Access Workstation
PCAP	Packet Capture

PIM	Privileged Identity Management
PIN	Personal Identification Number
PKCS	Public Key Cryptography Standards
PLC	Programmable Logic Controller
PPS	Pulse Per Second
PTP	Precision Time Protocol
PXE	Preboot Execution Environment
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RF	Radio Frequency
RHCP	Right-Hand Circular Polarization
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SAST	Static Application Security Testing
SBOM	Software Bill of Materials
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Network
SDR	Software Defined Radio
SELinux	Security-Enhanced Linux
SIEM	Security Information and Event Manager
SLE	Space Link Extension
SLSA	Supply-chain Levels for Software Artifacts

SMB	Server Message Block
SNMP	Simple Network Management Protocol
SOAR	Security Orchestration, Automation and Response
SOC	Security Operations Center
SP	Special Publication
SSH	Secure Shell
SSO	Single Sign-On
STIG	Security Technical Implementation Guide
STIX	Structured Threat Information Expression
TAP	Test Access Point
TAXII	Trusted Automated Exchange of Indicator Information
TC	Telecommand
TFTP	Trivial File Transfer Protocol
TLE	Two-Line Element
TLS	Transport Layer Security
TM	Telemetry
TPM	Trusted Platform Module
TTP	Tactics, Techniques, and Procedures
TT&C	Telemetry, Tracking, and Command
UEBA	User and Entity Behavior Analytics
UPS	Uninterruptible Power Supply
USB	Universal Serial Bus
VESDA	Very Early Smoke Detection Apparatus

VLAN	Virtual Local Area Network
VNC	Virtual Network Computing
VPN	Virtual Private Network
WAF	Web Application Firewall
WIDS	Wireless Intrusion Detection System
WIPS	Wireless Intrusion Prevention System
WMI	Windows Management Instrumentation
WinRM	Windows Remote Management
WORM	Write Once, Read Many
WPA3	Wi-Fi Protected Access 3
XSS	Cross-Site Scripting
ZTNA	Zero Trust Network Access

Appendix F: Document References

1. CNSS Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, 29 July 2022
2. NASA, SP-20240014019, *Risk Management Handbook*, https://ntrs.nasa.gov/citations/20120000033
3. NIST, *Cybersecurity Framework 2.0*, February 26, 2024
4. NIST, FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004
5. NIST, IR 8401, *Satellite Ground Segment - Applying the Cybersecurity Framework to Satellite Command and Control*, December 2022
6. NIST, SP 800-30, *Guide for Conducting Risk Assessments*, September 2012
7. NIST, SP 800-37 Revision 2, Risk Management Framework for Information Systems and Organizations, December 2018
8. NIST, SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View*, March 2011
9. NIST, SP 800-53 Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, September 2020
10. NIST, SP 800-53B, *Control Baselines for Information Systems and Organizations*, October 2020
11. NIST, SP 800-60 Volume I, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
12. NIST, SP 800-60 Volume II, *Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008
13. NIST, SP 800-161 Revision 1 Update 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, November 1, 2024
14. Office of Management and Budget, *Circular No. A-130: Managing Information as a Strategic Resource*, July 2016
15. Office of Management and Budget, Memoranda 19-03, *Strengthening the Cybersecurity of Federal Agencies by Enhancing the High Value Asset Program*, December 10, 2018
16. The Aerospace Corporation, *Cybersecurity Protections for Spacecraft: A Threat Based Approach,* TOR-2021-01333 Revision A, April 29, 2021
17. U.S. Congress, Title 44, U.S. Code §3505
18. U.S. Congress, *FISMA – Public Law 107-347,* 2002
19. U.S. Congress, *FISMA – Public Law 113-283*, 2014

Ground System Cyber Defenses and Risk-Based Tiering

Cognizant Program Manager Approval:

Danielle V. Bernstein, PRINCIPAL DIRECTOR
FEDERAL & COMMERCIAL PROGRAMS
CIVIL SYSTEMS OPERATIONS
CIVIL SYSTEMS GROUP

Export Control Office Approval Granted Electronically by:

Angela M. Farmer, SECURITY MANAGER
SECURITY OPERATIONS
ENTERPRISE PROTECTION & RESILIENCE
OFFICE OF THE CHIEF INFORMATION OFFICER