#### 4.2 Protect Function

The Protect Function includes development, implementation, and verification measures to prevent the loss of functionality in the SOC. Additionally, the Protect Function enables the response to and recovery from cybersecurity events with planning and preparation activities, while the execution of risk mitigation is addressed in the Response and Recovery Functions.

The objectives of the Protect Function include:

* Protect the systems that format and transmit commands to the required level of integrity, availability, and confidentiality.
* Protect the systems that receive and process telemetry, state of health or other data from the satellite or payload.
* Should a threat be realized, protect the space segment by enabling them to maintain a sufficient level of operations through verified response and recovery plans.

The Protect Function defines six Categories, all of which are applicable to the SOC to varying degrees, as summarized in Sections 4.2.1 through 4.2.6.

##### 4.2.1 Access Control Category

Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices and is managed consistent with the assessed risk of unauthorized access to authorized activities. In the context of the SOC, assets may include antennas, receivers, servers, and “physical access” may include radio frequency emanations.

There are seven Subcategories within Access Control, six of which apply to the SOC.

| Protect: Access Control | | |
| --- | --- | --- |
| Subcategory | Applicability to SOC | References |
| AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users, and processes. | Revoke credentials when the authorization of operators, devices, and processes expire or is no longer needed. | **NIST SP 800-53 Rev. 5** IA-1, IA-2, IA-3, IA-4, IA-5, IA-7, IA-8, IA-10, IA-11, IA-12 |
| PR.AC-2: Physical access to assets is managed and protected | Limit physical access to the SOC workstations to the greatest extent practical. Pre-define physical access for normal operations and for emergency situations.  Restrict physical access to antennas and monitor the RF environment. | **NIST SP 800-53 Rev. 5** PE-1, PE-2, PE-3, PE-4, PE-5, PE-6, PE-8, PE-9 |
| PR.AC-3: Remote access is managed | Connections to the SOC is strictly managed and SOC components that directly communicate with the space segment are typically air gapped.  Remote access is atypical but may be a part of an organization’s emergency response. If implemented, remote access is strictly limited to a subset of personnel using machines that are directly controlled and maintained by the organization. . | **NIST SP 800-53 Rev. 5** AC-1, AC-17, AC19, AC-20, SC-15 |
| PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties | Configure workstations and devices such that their functionality is limited to perform tasks associated with satellite operations. Consider mandatory access controls coupled with discretionary access controls to limit the authorization of an authenticated user. Consider granular role-based access controls such that an authenticated user’s authorization is limited to their assigned tasks and responsibilities.  Pre-define access and authorization controls for normal operations and for emergency situations. | **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC5, AC-6, AC-14, AC-16, AC-24  **NIST SP 800-160 Rev. 1** Appendix F.1.14 |
| PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) | Consider cryptographic isolation of payload commands that are tunneled through the satellite bus commands.  Command uplinks are typically encrypted and authenticated. Each command should have an associated nonce. Telemetry downlinks are often encrypted to provide isolation.  Separate C2, response, state of health and user traffic. If practical, consider cryptographic isolation of the user, control and management planes. | **NIST SP 800-53 Rev. 5** AC-4, SC-7, SC-10 |
| PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions | Verify the identity to the appropriate level of assurance prior to issuing of credentials. When validating credentials, consider contextual information such as geographic location, normal duty hours, task(s) being executed relative to normal tasking etc. | **ATIS-I-0000070** 2-7  **NISTIR 8014** 4-6  **NIST SP 800-53 Rev. 5** AC-1, AC-2, AC-3, AC16, AC-19, AC-24, IA-1, IA-2, IA-4, IA5, IA-8, IA-12, PE-2, PS-3 |
| PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the transaction (e.g., individuals’ security and privacy risks and other organizational risks) | SOC require physical access and authentication when initiating a session to the workstations within the SOC. Satellite uplinks and downlinks are encrypted at the transmission and receiver points. Authentication procedures take place during the key management and key rotation phases.  Authentication on a per transaction basis is atypical and not applicable for a typical SOC. | **IETF 4082** 2-5  **IETF 7822** 2-4 |

##### 4.2.2 Awareness and Training Category

The organization’s personnel and partners are provided cybersecurity awareness education and trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements. The awareness and training category is not unique to the satellite industry. The focus is on privileged users who operate, monitor and maintain equipment that interface with the space segment and third-party partners does not apply for bus and payload commanding/

There are five Subcategories within Awareness and Training, four of which apply to the SOC.

| Protect: Awareness and Training | | |
| --- | --- | --- |
| Subcategory | Applicability to SOC | References |
| PR.AT-1: All users are informed and trained. | Directly applies to SOC personnel for the bus and payload. | **NIST SP 800-53 Rev. 5**, AT-2, PM-13, PM-14 |
| PR.AT-2: Privileged users understand their roles and responsibilities. | Directly applies to SOC personnel for the bus and payload. Organizations will need to provide more specialized training in accordance with the granularity of the authorization and operation policies. | **NIST SP 800-53 Rev. 5** AT-3, PM-13  **NIST SP 800-160** Appendix E  1.7.8 |
| PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities. | Does not apply to SOC for either bus or payload. | **NIST SP 800-53 Rev. 5**, AT-3, PS-7, SA-9 |
| PR.AT-4: Senior executives understand their roles and responsibilities. | Directly applies to SOC personnel for the bus and payload. This is especially relevant in emergency scenarios. SOC tend to have granular authorization processes and procedures In the event of a crisis or emergency, senior executives will need to override processes for expediency’s sake. | **NIST SP 800-53 Rev. 5**, AT-3, PM-13 |
| PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities. | Directly applies to SOC personnel for the bus and payload. | **NIST SP 800-53 Rev. 5**, AT-3, CP-3, IR-2, PM-13 |

##### 4.2.3 Data Security Category

Information and data are managed consistent with the organization’s risk strategy to protect the confidentiality, integrity, and availability of commands, responses and telemetry. In the context of the SOC, the availability and integrity of commands are of primary concern.

There are eight Subcategories within Data Security, all of which apply to the SOC.

| Protect: Data Security | | |
| --- | --- | --- |
| Subcategory | Applicability to SOC | References |
| PR.DS-1: Data-at-rest is protected. | All TT&C data will need to be archived for at least the life of the satellite. The integrity of log and archive data will be especially important in forensic work. Apply measures such as access control lists, encryption, and other data-at-rest protections commensurate with the criticality of the activities.  Satellites are high value assets. Violation of an orbital position or a collision could have international implications therefore maintaining the integrity and availability of log and forensic data is paramount. | **GPS ICD-870** 3.3, 3.3.1  **NIST CSF** Appendix A CT.DP-P1-CT.DPP4  **NIST SP 800-37** 3  **NIST SP 800-53 Rev. 5** MP-3, MP-4, MP-6, SC-28 |
| PR.DS-2: Data-in-transit is protected. | The RF environment experiences interference and space assets are subject to a significant free space path loss and propagation delay which will impact the data-in-transit protection measures for the SOC. Use encryption and transmission security in accordance with availability and integrity requirements. | **NIST SP 800-53 Rev. 5** SC-8, SC-11, SC12 |
| PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition. | Many of the asset management requirements can be met by implementing solutions that provide the hardware inventory, software inventory and development life cycle management functions. Media sanitization and zeroization of crypto-variables warrants special consideration. | **NIST SP 800-53 Rev. 5** CM-8, MP-6, PE-16, PE-20 |
| PR.DS-4: Adequate capacity to ensure availability is maintained. | Commands, response, and telemetry tend to be low bandwidth operations and availability constraints are due to RF environmental events. This function is not particularly applicable within the SOC itself. | IEC 62439-3 4, 5 Appendix P.2.3 4.6, 4.8, 4.9, 4.12, 4.13  **NIST SP 800-53 Rev. 5** AU-4, CP-2, PE-11, SC-5  NIST SP 800-160 Appendix F.4 |
| PR.DS-5: Protections against data leaks are implemented. | Within a SOC, these protections are normally provided by other functions. Typical SOCs are air gapped or access is strictly controlled. Data-in-transit is normally encrypted. | **NIST SP 800-53 Rev. 5** AC-4, AC-5, AC-6, PE19, PS-3, PS-6, SC-7, SC-8, SC-13, SC31, SI-4,  **GPS ICD-240** |
| PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity. | Within a SOC, these protections are normally provided by other functions. The pedigree of software and firmware is addressed in the asset management category. Encryption (with a nonce) provides information integrity. | **GPS ICD-240**  **NIST SP 800-53 Rev. 5** SI-7, SI-10  **NIST SP 800-160 Rev. 1** 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F |
| PR.DS-7: The development and testing environment(s) are separate from the production environment. | Directly applicable for any SOC interacting with a bus or payload. Satellites are high value assets and technologies should be at TRL-7 prior to introduction to the SOC. | **NIST SP 800-53 Rev. 5** SI-7, SI-10 NIST SP 800-160 Rev. 1 2.3, 3.3.6, 3.4.9-3.4.11, Appendix F |
| PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity. | Within a SOC, this protection is normally provided by other functions, especially the asset management category. | **NISTIR 8320**  **NIST SP 800-53 Rev. 5** PE-11, SA-10, SI-7 |

##### 4.2.4 Information Protection Processes and Procedures Category

Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage the protection of information systems and assets.

There are twelve Subcategories within Information Protection Processes and Procedures, eleven of which apply to the SOC.

| Protect: Information Protection Processes and Procedures | | |
| --- | --- | --- |
| Subcategory | Applicability to SOC | References |
| PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality). | Especially germane to the SOC. In most cases, it is not practical to upgrade the space segment and the concept of least functionality can avoid unforeseen interactions. Install and configure devices and components per manufacturer instructions using established best practices. Understand the limitations of the original equipment manufacturer equipment being fielded and verify that devices and components are suitable.  Configure the SOC in a manner such that only essential capabilities are provided can reduce complexity, reduce the attack surface, and impact recovery time.  Verify that the baseline configuration results in a system that meets the baseline performance requirements, such as delay, wander, and jitter tolerances. | **NIST SP 800-53 Rev. 5** CM-1, CM-2, CM3, CM-4, CM5, CM-6, CM-7, CM-9, SA-10  **NIST SP 800-160** 3.4.9, 3.4.10, 3.4.11 Appendix F, G  **RTCA 235** |
| PR.IP-2: A System Development Life Cycle to manage systems is implemented. | Incorporate and manage security measures throughout the life cycle of components. Document the requirements, approach, architectures, and assumptions used to minimize risks for systems.  Consider the intended lifetime of the systems that that are dependent on the SOC and be aware that systems nearing end of life may have parts/ components obsolescence or availability issues. | **NIST CSF** Appendix A CT.PO-P4  **NIST SP 800-53 Rev. 5** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17  **NIST SP 800-160 Rev. 1** 3.2.1, Appendix F.3 |
| PR.IP-3: Configuration change control processes are in place. | Employ configuration change control for the SOC and its components that are consistent with the software development life cycle to maintain a functioning baseline and monitor all changes to validate impacts and integrity. Prior to deploying a change, conduct impact analyses.  Provide a mechanism so that changes in SOC firmware and software can be returned to a proper working state. | **NIST SP 800-53 Rev. 5** CM-3, CM-4, SA10  **NIST SP 800-160 Rev. 1** 3.3.5, 3.8.3, 3.8.4 |
| PR.IP-4: Backups of information are conducted, maintained, and tested. | Within a SOC, this function is typically provided as a part of other sub-categories, especially PR.IP.-9 and 10. Space enterprises typically have one or more redundant facilities that include transmitters, receivers, workstations that that generate commands, process telemetry etc. | **NIST SP 800-53 Rev. 5**, CP-4, CP-6, CP-9 |
| PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met. | Not directly applicable to the SOC. | **NIST SP 800-53 Rev. 5**, PE-1 |
| PR.IP-6: Data is destroyed according to policy | Not directly applicable to the SOC. Telemetry, commands, response data is retained for future analysis and forensics. | **NIST SP 800-53 Rev. 5**, MP-6, SR-12 |
| PR.IP-7: Protection processes are improved. | No SOC specific considerations. | **NIST SP 800-53 Rev. 5**, CA-2, CA-7, CA-8, CP-2, CP-4, IR-3, IR-8, PL-2, PM-6 |
| PR.IP-8: Effectiveness of protection technologies is shared. | Not directly applicable to the SOC. A large fraction of the components and systems within the SOC are custom for space operations which is a niche use case (relative to other cyber operations). Efficacy of protection technologies is not necessarily applicable to other organizations. | **NIST SP 800-53 Rev. 5**, AC-21, CA-7, CP-2, IR-8, SI-4 |
| PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed. | Especially germane to SOC. Space assets are high cost/ value assets that are inaccessible and have a limited ability to act autonomously. Response and business continuity plans need to be executed in a manner that is consistent with the space segment’s ability to operate in an autonomous safe mode and in the case of a congested orbital slot, in a manner to avoid collisions.  Develop and maintain response and recovery plans that identify essential functions and associated contingency requirements, as well as provide a roadmap for implementing incident response. Plans should incorporate recovery objectives, restoration priorities, tests, metrics, contingency roles, personnel assignments, and contact information. Prioritize maintaining essential functions despite system disruption or manipulation, as well as the eventual restoration to normal operations. | **IEC 61850-90-12** 5.8 4.12-4.14  **NIST SP 800-53 Rev. 5** CP-1, CP-2, CP-7, CP-10, CP-12, CP13, IR-1, IR-7, IR-8, IR-9, PE-17  **NIST SP 800-160 Rev.1** Appendix F.2.6 5.6.6 |
| PR.IP-10: Response and recovery plans are tested. | Assess preparedness by verifying incident response and recovery plans. Consider qualification and periodic testing to assess the response and recovery plans as the satellites age or changes to space operations that would significantly impact the performance requirements for the SOC. Review the results to determine the efficiency and effectiveness of the plans as well as readiness to execute the plans. Use the results of the tests to inform other CSF functions, such as “Detect.”  Exercise the response and recovery plans to validate that the effects of an incident on the command link’s availability, integrity, and continuity are within specified tolerances. | **IEC 61850-90-4** 14.2.4 5.4.2.5  **NERC GridEx**  **NIST SP 800-53 Rev. 5** CP-4, IR-3, PM-14 |
| PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening). | Highly critical SOC operations *may* warrant measures such as two-person-integrity, otherwise no SOC specific considerations. | **NIST SP 800-53 Rev. 5**, PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, PS-9, SA-21 |
| PR.IP-12: A vulnerability management plan is developed and implemented. | No SOC specific considerations | **NIST SP 800-53 Rev. 5**, RA-1, RA-3, RA-5, SI-2 |

##### 4.2.5 Maintenance Category

Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.

There are two Subcategories within the Maintenance Category one of which applies to the SOC.

| Protect: Maintenance | | |
| --- | --- | --- |
| Subcategory | Applicability to SOC | References |
| PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools | Schedule, perform, record, and review records of maintenance and repairs at the SOC.  Assess the impacts of the maintenance and repair of the SOC devices and components on the satellite bus and payload operations and verify their performance within specified tolerances.  Make available and adhere to documentation and artifacts, such as software maintenance procedures, configuration parameters (including default values and ranges), test plans, compliance test result documentation, and other pertinent information to ensure consistent and valid operations. | **NIST SP 800-53 Rev. 5** MA-1, MA-2, MA3, MA-5, MA-6 |
| PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access | Normally not applicable to the SOC. Typical SOCs will have permanent virtual circuits, implement a VPN or have prearranged and preconfigured connections to the vendor. Use temporary remote logins are atypical in a SOC. | **NIST SP 800-53 Rev. 5** MA-4  **NIST SP 800-160 Rev. 1** Appendix F.1.14 |

##### 4.2.6 Protective Technology Category

Technical security solutions are managed to ensure the security and resilience of systems and assets consistent with related policies, procedures, and agreements.

There are five Subcategories within the Protective Technology Category, all of which apply to the SOC.

| Protect: Protective Technology | | |
| --- | --- | --- |
| Subcategory | Applicability to SOC | References |
| PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy. | Space faring operations may have a legal requirement to maintain an unbroken documented chain of events for audit purposes. A log file may be required to include entries of proper working states in addition to entries of anomalies and events.  Wherever practical, logging and audit mechanisms should produce data elements in accordance with standard data formats to facilitate parsing and consumption by analytic teams.  Consider maintaining audit logs for extended periods to support forensic analysis. | **NIST SP 800-53 Rev. 5** AU-1, AU-2, AU-3, AU-6, AU-7, AU-12, AU-13, AU-14, AU16  **NIST SP 800-160 Rev. 1** 3.3.2, 3.3.5 |
| PR.PT-2: Removable media is protected and its use restricted according to policy. | Not applicable to typical SOCs. Policies will prohibit the routine use of removable media.  Ensure devices and equipment follow organizational policy on the use of portable media and employ safeguards to enforce the restriction of the use of portable media. | **NIST SP 800-53 Rev. 5** MP-1, MP-2, MP-3, MP-4, MP5, MP-7, MP-8 |
| PR. PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities. | Configure the SOC system’s hardware and software to only provide essential capabilities.  Disabled functionality will minimize attack surfaces and facilitate detection. | **NIST SP 800-53 Rev. 5** AC-3, CM-7 |
| PR.PT-4: Communications and control networks are protected. | The SOC has a high availability and integrity requirements.  Some measures need to be considered at the architectural phase of the SDLC, such as TRANSEC implementations (typically at the physical layer) while others can be applied at the configuration or deployment phase, such as transport security (typically at layer 3 and above).  Note that implementing some security measures can lead to performance degradation that may be problematic. Verify that protective measures will not adversely affect the overall system performance requirements. | **NIST CSF** PR.PT-P3  **NIST SP 800-53 Rev. 5** AC-12, AC-17, AC-18, CP-8, SC-5, SC-7, SC-10, SC-11, SC-20, SC-21, SC-22, SC-23, SC-31, SC-37, SC-38, SC-47  **NIST SP 800-160 Rev. 1** Appendix F |
| PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations | The duration that a space vehicle may operate autonomously defines the lower bound of resilience requirements. Typical SOCs have hot swap within the facility and have hot swap alternate facilities. Measures should be present to handle attacks that penetrate into SOC systems, including holdover capabilities paired with anomaly detection, features to limit performance degradation, and recovery capabilities. | **NIST SP 800-53 Rev. 5** CP-7, CP-8, CP-11, CP-12, CP-13, PE-11, PL-8, SC-6 |