Set Theory Relationship Mapping (STRM)

Reference Document : Secure Controls Framework (SCF) version 2024.2
Focal Document: Space Attack Research and Tactic Analysis (SPARTA)
Focal Document URL: https://sparta.aerospace.org/countermeasures/SPARTA
STRM URL: https://content.securecontrolsframework.com/strm/scf-2024-2-sparta.pdf

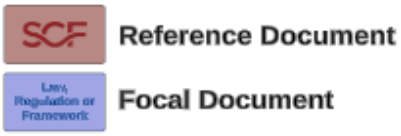
Set Theory Relationship Mapping (STRM) is well-suited for mapping between sets of elements that exist in two distinct concepts that are mostly the same as each other (e.g., cybersecurity & data privacy requirements). STRM also allows the strength of the mapping to be captured.

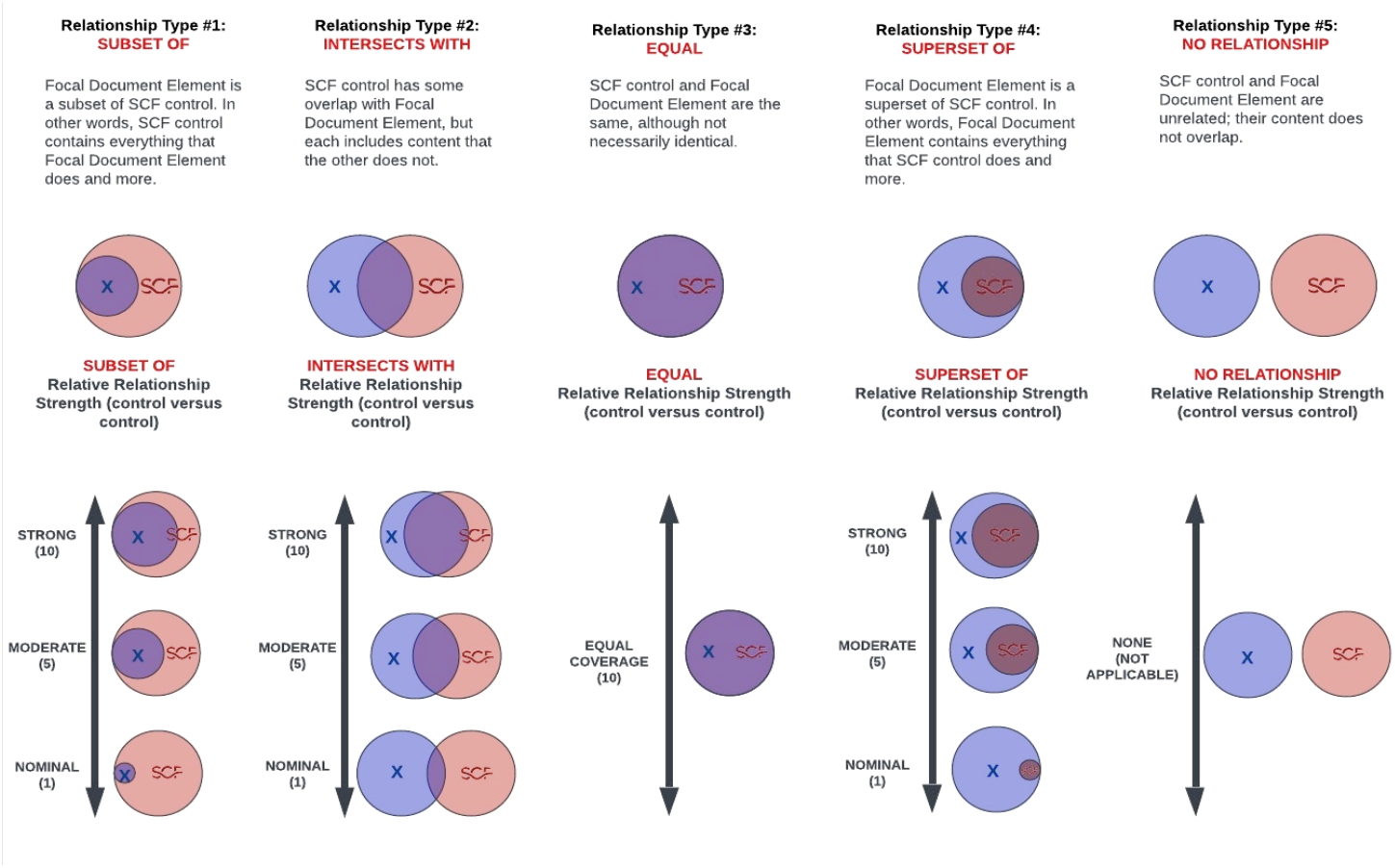
STRM relies on a justification for the relationship claim. There are three (3) options for the rationale, which is a high-level context within which the two concepts are related:

1. **Syntactic**: How similar is the wording that expresses the two concepts? This is a word-for-word analysis of the relationship, not an interpretation of the language.
2. **Semantic**: How similar are the meanings of the two concepts? This involves some interpretation of each concept's language.
3. **Functional**: How similar are the results of executing the two concepts? This involves understanding what will happen if the two concepts are implemented, performed, or otherwise executed.

Based on NIST IR 8477, STRM supports five (5) five relationship types to describe the logical similarity between two distinct concepts:

1. **Subset Of**
2. **Intersects With**
3. **Equal**
4. **Superset Of**
5. **No Relationship**





FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CM0000	Countermeasure Not Identified	This technique is a result of utilizing TTPs to create an impact and the applicable countermeasures are associated with the TTPs leveraged to achieve the impact	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0001	Protect Sensitive Information	Organizations should look to identify and properly classify mission sensitive design/operations information (e.g., fault management approach) and apply access control accordingly. Any location (ground system, contractor networks, etc.) storing design information needs to ensure design info is protected from exposure, exfiltration, etc. Space system sensitive information may be classified as Controlled Unclassified Information (CUI) or Company Proprietary. Space system sensitive information can typically include a wide range of candidate material: the functional and performance specifications, any ICDs (like radio frequency, ground-to-space, etc.), command and telemetry databases, scripts, simulation and rehearsal results/reports, descriptions of uplink protection including any disabling/bypass features, failure/anomaly resolution, and any other sensitive information related to architecture, software, and flight/ground /mission operations. This could all need protection at the appropriate level (e.g., unclassified, CUI, proprietary, classified, etc.) to mitigate levels of cyber intrusions that may be conducted against the project's networks. Stand-alone systems and/or	Functional	intersects with	Asset Scope Classification	AST-04.1	Mechanisms exist to determine cybersecurity & data privacy control applicability by identifying, assigning and documenting the appropriate asset scope categorization for all systems, applications, services and personnel (internal and third-parties).	5	
			Functional	intersects with	Data Protection	DCH-01	Mechanisms exist to facilitate the implementation of data protection controls.	5	
			Functional	intersects with	Sensitive / Regulated Data Protection	DCH-01.2	Mechanisms exist to protect sensitive/regulated data wherever it is stored.	5	
			Functional	intersects with	Data & Asset Classification	DCH-02	Mechanisms exist to ensure data and assets are categorized in accordance with applicable statutory, regulatory and contractual requirements.	5	
CM0002	COMSEC	A component of cybersecurity to deny unauthorized persons information derived from telecommunications and to ensure the authenticity of such telecommunications. COMSEC includes cryptographic security, transmission security, emissions security, and physical security of COMSEC material. It is imperative to utilize secure communication protocols with strong cryptographic mechanisms to prevent unauthorized disclosure of, and detect changes to, information during transmission. Systems should also maintain the confidentiality and integrity of information during preparation for transmission and during reception. Spacecraft should not employ a mode of operations where cryptography on the TT&C link can be disabled (i.e., crypto-bypass mode). The cryptographic mechanisms should identify and reject wireless transmissions that are deliberate attempts to achieve imitative or manipulative communications deception based on signal parameters.	Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
CM0003	TEMPEST	The spacecraft should protect system components, associated data communications, and communication buses in accordance with TEMPEST controls to prevent side channel / proximity attacks. Encompass the spacecraft critical components with a casing/shielding so as to prevent access to the individual critical components.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0004	Development Environment Security	In order to secure the development environment, the first step is understanding all the devices and people who interact with it. Maintain an accurate inventory of all people and assets that touch the development environment. Ensure strong multi-factor authentication is used across the development environment, especially for code repositories, as threat actors may attempt to sneak malicious code into software that's being built without being detected. Use zero-trust access controls to the code repositories where possible. For example, ensure the main branches in repositories are protected from injecting malicious code. A secure development environment requires change management, privilege management, auditing and in-depth monitoring across the environment.	Functional	intersects with	Secure Development Environments	TDA-07	Mechanisms exist to maintain a segmented development network to ensure a secure development environment.	5	
CM0005	Ground-based Countermeasures	This countermeasure is focused on the protection of terrestrial assets like ground networks and development environments/contractor networks, etc. Traditional detection technologies and capabilities would be applicable here. Utilizing resources from NIST CSF to properly secure these environments using identify, protect, detect, recover, and respond is likely warranted. Additionally, NISTIR 8401 may provide resources as well since it was developed to focus on ground-based security for space systems (https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf). Furthermore, the MITRE ATT&CK framework provides IT focused TTPs and their mitigations https://attack.mitre.org/mitigations/enterprise/. Several recommended NIST 800-53 Rev5 controls are provided for reference when designing ground systems/networks.	Functional	intersects with	Cybersecurity & Data Protection Governance Program	GOV-01	Mechanisms exist to facilitate the implementation of cybersecurity & data protection governance controls.	5	
CM0006	Cloaking Safe-mode	Attempt to cloak when in safe-mode and ensure that when the system enters safe-mode it does not disable critical security features. Ensure basic protections like encryption are still being used on the uplink/downlink to prevent eavesdropping.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0007	Software Version Numbers	When using COTS or Open-Source, protect the version numbers being used as these numbers can be cross referenced against public repos to identify Common Vulnerability Exposures (CVEs) and exploits available.	Functional	intersects with	Commercial Off-The-Shelf (COTS) Security Solutions	TDA-03	Mechanisms exist to utilize only Commercial Off-the-Shelf (COTS) security products.	5	
			Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CM0008	Security Testing Results	As penetration testing and vulnerability scanning is a best practice, protecting the results from these tests and scans is equally important. These reports and results typically outline detailed vulnerabilities and how to exploit them. As with countermeasure CM0001, protecting sensitive information from disclosure to threat actors is imperative.	Functional	intersects with	Penetration Testing	VPM-07	Mechanisms exist to conduct penetration testing on systems and web applications.	5	
			Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
CM0009	Threat Intelligence Program	A threat intelligence program helps an organization generate their own threat intelligence information and track trends to inform defensive priorities and mitigate risk. Leverage all-source intelligence services or commercial satellite imagery to identify and track adversary infrastructure development/acquisition. Countermeasures for this attack fall outside the scope of the mission in the majority of cases.	Functional	intersects with	Threat Intelligence Program	THR-01	Mechanisms exist to implement a threat intelligence program that includes a cross-organization information-sharing capability that can influence the development of the system and security architectures, selection of security solutions, monitoring, threat hunting, response and recovery activities.	5	
CM0010	Update Software	Perform regular software updates to mitigate exploitation risk. Software updates may need to be scheduled around operational down times. Release updated versions of the software/firmware systems incorporating security-relevant updates, after suitable regression testing, at a frequency no greater than mission-defined frequency [i.e., 30 days]. Ideally old versions of software are removed after upgrading but restoration states (i.e., gold images) are recommended to remain on the system.	Functional	intersects with	Software & Firmware Patching	VPM-05	Mechanisms exist to conduct software patching for all deployed operating systems, applications and firmware.	5	
CM0011	Vulnerability Scanning	Vulnerability scanning is used to identify known software vulnerabilities (excluding custom-developed software - ex: COTS and Open-Source). Utilize scanning tools to identify vulnerabilities in dependencies and outdated software (i.e., software composition analysis). Ensure that vulnerability scanning tools and techniques are employed that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for: (1) Enumerating platforms, custom software flaws, and improper configurations; (2) Formatting checklists and test procedures; and (3) Measuring vulnerability impact.	Functional	intersects with	Vulnerability Scanning	VPM-06	Mechanisms exist to detect vulnerabilities and configuration errors by routine vulnerability scanning of systems and applications.	5	
CM0012	Software Bill of Materials	Generate Software Bill of Materials (SBOM) against the entire software supply chain and cross correlate with known vulnerabilities (e.g., Common Vulnerabilities and Exposures) to mitigate known vulnerabilities. Protect the SBOM according to countermeasures in CM0001.	Functional	intersects with	Software Bill of Materials (SBOM)	TDA-04.2	Mechanisms exist to generate, or obtain, a Software Bill of Materials (SBOM) for systems, applications and services that lists software packages in use, including versions and applicable licenses.	5	
CM0013	Dependency Confusion	Ensure proper protections are in place for ensuring dependency confusion is mitigated like ensuring that internal dependencies be pulled from private repositories vice public repositories, ensuring that your CI/CD/development environment is secure as defined in CM0004 and validate dependency integrity by ensuring checksums match official packages.	Functional	intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
CM0014	Secure boot	Software/Firmware must verify a trust chain that extends through the hardware root of trust, boot loader, boot configuration file, and operating system image, in that order. The trusted boot/RoT computing module should be implemented on radiation tolerant burn-in (non-programmable) equipment.	Functional	intersects with	Protection of Boot Firmware	END-06.6	Automated mechanisms exist to protect the integrity of boot firmware in information systems.	5	
			Functional	intersects with	Boot Process Integrity	END-06.5	Automated mechanisms exist to verify the integrity of the boot process of information systems.	5	
CM0015	Software Source Control	Prohibit the use of binary or machine-executable code from sources with limited or no warranty and without the provision of source code.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0016	CWE List	Create prioritized list of software weakness classes (e.g., Common Weakness Enumerations), based on system-specific considerations, to be used during static code analysis for prioritization of static analysis results.	Functional	intersects with	Vulnerability Ranking	VPM-03	Mechanisms exist to identify and assign a risk ranking to newly discovered security vulnerabilities using reputable outside sources for security vulnerability information.	5	
			Functional	intersects with	Vulnerability Exploitation Analysis	VPM-03.1	Mechanisms exist to identify, assess, prioritize and document the potential impact(s) and likelihood(s) of applicable internal and external threats exploiting known vulnerabilities.	5	
			Functional	intersects with	Vulnerability & Patch Management Program (VPMP)	VPM-01	Mechanisms exist to facilitate the implementation and monitoring of vulnerability management controls.	5	
CM0017	Coding Standard	Define acceptable coding standards to be used by the software developer. The mission should have automated means to evaluate adherence to coding standards. The coding standard should include the acceptable software development language types as well. The language should consider the security requirements, scalability of the application, the complexity of the application, development budget, development time limit, application security, available resources, etc. The coding standard and	Functional	intersects with	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of systems, applications and services.	5	
			Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
CM0018	Dynamic Analysis	Employ dynamic analysis (e.g., using simulation, penetration testing, fuzzing, etc.) to identify software/firmware weaknesses and vulnerabilities in developed and incorporated code (open source, commercial, or third-party developed code). Testing should occur (1) on potential system elements before acceptance; (2) as a realistic simulation of known adversary tactics, techniques, procedures (TTPs), and tools; and (3) throughout the lifecycle on physical and logical systems, elements, and processes. FLATSATs as well as digital twins can be used to perform the dynamic analysis depending on the TTPs being executed. Digital twins via instruction set simulation (i.e., emulation) can provide robust environment for dynamic analysis and TTP execution.	Functional	intersects with	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
CM0019	Static Analysis	Perform static source code analysis for all available source code looking for system-relevant weaknesses (see CM0016) using no less than two static code analysis tools.	Functional	intersects with	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
CM0020	Threat modeling	Use threat modeling, attack surface analysis, and vulnerability analysis to inform the current development process using analysis from similar systems, components, or services where applicable. Reduce attack surface where possible based on threats.	Functional	intersects with	Threat Modeling	TDA-06.2	Mechanisms exist to perform threat modelling and other secure design techniques, to ensure that threats to software and solutions are identified and accounted for.	5	
CM0021	Software Digital Signature	Prevent the installation of Flight Software without verification that the component has been digitally signed using a certificate that is recognized and approved by the mission.	Functional	intersects with	Signed Components	CHG-04.2	Mechanisms exist to prevent the installation of software and firmware components without verification that the component has been digitally signed using an organization-approved certificate authority.	5	
			Functional	intersects with	Criticality Analysis	TDA-06.1	Mechanisms exist to require the developer of the system, system component or service to perform a criticality analysis at organization-defined decision points in the Secure Development Life Cycle (SDLC).	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CM0022	Criticality Analysis	Conduct a criticality analysis to identify mission critical functions, critical components, and data flows and reduce the vulnerability of such functions and components through secure system design. Focus supply chain protection on the most critical components/functions. Leverage other countermeasures like segmentation and least privilege to protect the critical components.	Functional	intersects with	Asset-Service Dependencies	AST-01.1	Mechanisms exist to identify and assess the security of technology assets that support more than one critical business function.	5	
			Functional	intersects with	Network Diagrams & Data Flow Diagrams (DFDs)	AST-04	Mechanisms exist to maintain network architecture diagrams that: • Contain sufficient detail to assess the security of the network's architecture; • Reflect the current architecture of the network environment; and • Document all sensitive/regulated data flows.	5	
			Functional	intersects with	Asset Categorization	AST-31	Mechanisms exist to categorize technology assets.	5	
			Functional	intersects with	Third-Party Criticality Assessments	TPM-02	Mechanisms exist to identify, prioritize and assess suppliers and partners of critical systems, components and services using a supply chain risk assessment process relative to their importance in supporting the delivery of high-value services.	5	
CM0023	Configuration Management	Use automated mechanisms to maintain and validate baseline configuration to ensure the spacecraft's is up-to-date, complete, accurate, and readily available.	Functional	intersects with	Configuration Management Program	CFG-01	Mechanisms exist to facilitate the implementation of configuration management controls.	5	
			Functional	intersects with	Automated Central Management & Verification	CFG-02.2	Automated mechanisms exist to govern and report on baseline configurations of systems through Continuous Diagnostics and Mitigation (CDM), or similar technologies.	5	
CM0024	Anti-counterfeit Hardware	Develop and implement anti-counterfeit policy and procedures designed to detect and prevent counterfeit components from entering the information system, including tamper resistance and protection against the introduction of malicious code or hardware.	Functional	intersects with	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
			Functional	intersects with	Anti-Counterfeit Training	TDA-11.1	Mechanisms exist to train personnel to detect counterfeit system components, including hardware, software and firmware.	5	
CM0025	Supplier Review	Conduct a supplier review prior to entering into a contractual agreement with a contractor (or sub-contractor) to acquire systems, system components, or system services.	Functional	intersects with	Third-Party Management	TPM-01	Mechanisms exist to facilitate the implementation of third-party management controls.	5	
			Functional	intersects with	Third-Party Risk Assessments & Approvals	TPM-04.1	Mechanisms exist to conduct a risk assessment prior to the acquisition or outsourcing of technology-related services.	5	
CM0026	Original Component Manufacturer	Components/Software that cannot be procured from the original component manufacturer or their authorized franchised distribution network should be approved by the supply chain board or equivalent to prevent and detect counterfeit and fraudulent parts, materials, and software.	Functional	intersects with	Supply Chain Risk Management (SCRM) Plan	RSK-09	Mechanisms exist to develop a plan for Supply Chain Risk Management (SCRM) associated with the development, acquisition, maintenance and disposal of systems, system components and services, including documenting selected mitigating actions and monitoring performance against those plans.	5	
			Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
			Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
CM0027	ASIC/FPGA Manufacturing	Application-Specific Integrated Circuit (ASIC) / Field Programmable Gate Arrays should be developed by accredited trusted foundries to limit potential hardware-based trojan injections.	Functional	intersects with	Supply Chain Protection	TPM-03	Mechanisms exist to evaluate security risks associated with the services and product supply chain.	5	
			Functional	intersects with	Acquisition Strategies, Tools & Methods	TPM-03.1	Mechanisms exist to utilize tailored acquisition strategies, contract tools and procurement methods for the purchase of unique systems, system components or services.	5	
CM0028	Tamper Protection	Perform physical inspection of hardware to look for potential tampering. Leverage tamper proof protection where possible when shipping/receiving equipment.	Functional	intersects with	Product Tampering and Counterfeiting (PTC)	TDA-11	Mechanisms exist to maintain awareness of component authenticity by developing and implementing Product Tampering and Counterfeiting (PTC) practices that include the means to detect and prevent counterfeit components.	5	
			Functional	intersects with	Tamper Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	
CM0029	TRANSEC	Utilize TRANSEC in order to prevent interception, disruption of reception, communications deception, and/or derivation of intelligence by analysis of transmission characteristics such as signal parameters or message externals. For example, jam-resistant waveforms can be utilized to improve the resistance of radio frequency signals to jamming and spoofing. Note: TRANSEC is that field of COMSEC which deals with the security of communication transmissions, rather than that of the information being communicated.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0030	Crypto Key Management	Leverage best practices for crypto key management as defined by organization like NIST or the National Security Agency. Leverage only approved cryptographic algorithms, cryptographic key generation algorithms or key distribution techniques, authentication techniques, or evaluation criteria. Encryption key handling should be performed outside of the onboard software and protected using cryptography. Encryption keys should be restricted so that they cannot be read via any telecommands.	Functional	intersects with	Cryptographic Key Management	CRY-09	Mechanisms exist to facilitate cryptographic key management controls to protect the confidentiality, integrity and availability of keys.	5	
CM0031	Authentication	Authenticate all communication sessions (crosslink and ground stations) for all commands before establishing remote connections using bidirectional authentication that is cryptographically based. Adding authentication on the spacecraft bus and communications on-board the spacecraft is also recommended.	Functional	intersects with	Identification & Authentication for Organizational Users	IAC-02	Mechanisms exist to uniquely identify and centrally Authenticate, Authorize and Audit (AAA) organizational users and processes acting on behalf of organizational users.	5	
			Functional	intersects with	Authenticate, Authorize and Audit (AAA)	IAC-01.2	Mechanisms exist to strictly govern the use of Authenticate, Authorize and Audit (AAA) solutions, both on-premises and those hosted by an External Service Provider (ESP).	5	
CM0032	On-board Intrusion Detection & Prevention	Utilize on-board intrusion detection/prevention system that monitors the mission critical components or systems and audit/logs actions. The IDS/IPS should have the capability to respond to threats (initial access, execution, persistence, evasion, exfiltration, etc.) and it should address signature-based attacks along with dynamic never-before seen attacks using machine learning/adaptive technologies. The IDS/IPS must integrate with traditional fault management to provide a wholistic approach to faults on-board the spacecraft. Spacecraft should select and execute safe countermeasures against cyber-attacks. These countermeasures are a ready supply of options to triage against the specific types of attack and mission priorities. Minimally, the response should ensure vehicle safety and continued operations. Ideally, the goal is to trap the threat, convince the threat that it is successful, and trace and track the attacker — with or without ground support. This would support successful attribution and evolving countermeasures to mitigate the threat in the future. "Safe countermeasures" are those that are compatible with the system's fault management system to avoid unintended effects or fratricide on the system.	Functional	intersects with	Intrusion Detection & Prevention Systems (IDS & IPS)	MON-01.1	Mechanisms exist to implement Intrusion Detection / Prevention Systems (IDS / IPS) technologies on critical systems, key network segments and network choke points.	5	
CM0033	Relay Protection	Implement relay and replay-resistant authentication mechanisms for establishing a remote connection or connections on the spacecraft bus.	Functional	intersects with	Network Security Controls (NSC)	NET-01	Mechanisms exist to develop, govern & update procedures to facilitate the implementation of Network Security Controls (NSC).	5	
CM0034	Monitor Critical Telemetry Points	Monitor defined telemetry points for malicious activities (i.e., jamming attempts, commanding attempts (e.g., command modes, counters, etc.)). This would include valid/processed commands as well as commands that were rejected. Telemetry monitoring should synchronize with ground-based Defensive Cyber Operations (i.e., SIEM/auditing) to create a full space system situation awareness from a cybersecurity perspective.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0035	Protect Authenticators	Protect authenticator content from unauthorized disclosure and modification.	Functional	intersects with	Protection of Authenticators	IAC-10.5	Mechanisms exist to protect authenticators commensurate with the sensitivity of the information to which use of the authenticator permits access.	5	
CM0036	Session Termination	Terminate the connection associated with a communications session at the end of the session or after an acceptable amount of inactivity which is established via the concept of operations.	Functional	intersects with	Session Termination	IAC-25	Automated mechanisms exist to log out users, both locally on the network and for remote sessions, at the end of the session or after an organization-defined period of inactivity.	5	
CM0037	Disable Physical Ports	Provide the capability for data connection ports or input/output devices (e.g., JTAG) to be disabled or removed prior to spacecraft operations.	Functional	intersects with	Interface Security	EMB-04	Mechanisms exist to protect embedded devices against unauthorized use of the physical factory diagnostic and test interface(s).	5	
			Functional	intersects with	Prevent Alterations	EMB-06	Mechanisms exist to protect embedded devices by preventing the unauthorized installation and execution of software.	5	
			Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
			Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
CM0038	Segmentation	Identify the key system components or capabilities that require isolation through physical or logical means. Information should not be allowed to flow between partitioned applications unless explicitly permitted by security policy. Isolate mission critical functionality from non-mission critical functionality by means of an isolation boundary (implemented via partitions) that controls access to and protects the integrity of, the hardware, software, and firmware that provides that functionality. Enforce approved authorizations for controlling the flow of information within the spacecraft and between interconnected systems based on the defined security policy that information does not leave the spacecraft boundary unless it is encrypted. Implement boundary protections to separate bus, communications, and payload components supporting their respective functions.	Functional	intersects with	Network Segmentation (macrosegementation)	NET-06	Mechanisms exist to ensure network architecture utilizes network segmentation to isolate systems, applications and services that protections from other network resources.	5	
CM0039	Least Privilege	Employ the principle of least privilege, allowing only authorized processes which are necessary to accomplish assigned tasks in accordance with system functions. Ideally maintain a separate execution domain for each executing process.	Functional	intersects with	Least Privilege	IAC-21	Mechanisms exist to utilize the concept of least privilege, allowing only authorized access to processes necessary to accomplish assigned tasks in accordance with organizational business functions.	5	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CM0040	Shared Resource Leakage	Prevent unauthorized and unintended information transfer via shared system resources. Ensure that processes reusing a shared system resource (e.g., registers, main memory, secondary storage) do not have access to information (including encrypted representations of information) previously stored in that resource during a prior use by a process after formal release of that resource back to the system or reuse	Functional	intersects with	Information In Shared Resources	SEA-05	Mechanisms exist to prevent unauthorized and unintended information transfer via shared system resources.	5	
CM0041	User Training	Train users to be aware of access or manipulation attempts by a threat actor to reduce the risk of successful spear phishing, social engineering, and other techniques that involve user interaction. Ensure that role-based security-related training is provided to personnel with assigned security roles and responsibilities: (i) before authorizing access to the information system or performing assigned duties; (ii) when required by information system changes; and (iii) at least annually if not otherwise defined.	Functional	intersects with	Role-Based Cybersecurity & Data Privacy Training	SAT-03	Mechanisms exist to provide role-based cybersecurity & data privacy-related training: • Before authorizing access to the system or performing assigned duties; • When required by system changes; and • Annually thereafter.	5	
			Functional	intersects with	Cyber Threat Environment	SAT-03.6	Mechanisms exist to provide role-based cybersecurity & data privacy awareness training that is current and relevant to the cyber threats that users might encounter in day-to-day business operations.	5	
			Functional	intersects with	Suspicious Communications & Anomalous System Behavior	SAT-03.2	Mechanisms exist to provide training to personnel on organization-defined indicators of malware to recognize suspicious communications and anomalous behavior.	5	
			Functional	intersects with	Sensitive Information Storage, Handling & Processing	SAT-03.3	Mechanisms exist to ensure that every user accessing a system processing, storing or transmitting sensitive information is formally trained in data handling requirements.	5	
CM0042	Robust Fault Management	Ensure fault management system cannot be used against the spacecraft. Examples include: safe mode with crypto bypass, orbit correction maneuvers, affecting integrity of telemetry to cause action from ground, or some sort of proximity operation to cause spacecraft to go into safe mode. Understanding the safing procedures and ensuring they do not put the spacecraft in a more vulnerable state is key to building a resilient spacecraft.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0043	Backdoor Commands	Ensure that all viable commands are known to the mission/spacecraft owner. Perform analysis of critical (backdoor/hardware) commands that could adversely affect mission success if used maliciously. Only use or include critical commands for the purpose of providing emergency access where commanding authority is appropriately restricted.	Functional	intersects with	Software Design Review	TDA-06.5	Mechanisms exist to have an independent review of the software design to confirm that all cybersecurity & data privacy requirements are met and that any identified risks are satisfactorily addressed.	5	
			Functional	intersects with	Software Assurance Maturity Model (SAMM)	TDA-06.3	Mechanisms exist to utilize a Software Assurance Maturity Model (SAMM) to govern a secure development lifecycle for the development of systems, applications and services.	5	
			Functional	intersects with	Dynamic Code Analysis	TDA-09.3	Mechanisms exist to require the developers of systems, system components or services to employ dynamic code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
			Functional	intersects with	Static Code Analysis	TDA-09.2	Mechanisms exist to require the developers of systems, system components or services to employ static code analysis tools to identify and remediate common flaws and document the results of the analysis.	5	
			Functional	intersects with	Secure Coding	TDA-06	Mechanisms exist to develop applications based on secure coding principles.	5	
CM0044	Cyber-safe Mode	Provide the capability to enter the spacecraft into a configuration-controlled and integrity-protected state representing a known, operational cyber-safe state (e.g., cyber-safe mode). Spacecraft should enter a cyber-safe mode when conditions that threaten the platform are detected. Cyber-safe mode is an operating mode of a spacecraft during which all nonessential systems are shut down and the spacecraft is placed in a known good state using validated software and configuration settings. Within cyber-safe mode, authentication and encryption should still be enabled. The spacecraft should be capable of reconstituting firmware and software functions to pre-attack levels to allow for the recovery of functional capabilities. This can be performed by self-healing, or the healing can be aided from the ground. However, the spacecraft needs to have the capability to replan, based on equipment still available after a cyber-attack. The goal is for the spacecraft to resume full mission operations. If not possible, a reduced level of mission capability should be achieved. Cyber-safe mode software/configuration should be stored onboard the spacecraft in memory with hardware-based controls and should not be modifiable.	Functional	intersects with	Fail Secure	SEA-07.2	Mechanisms exist to enable systems to fail to an organization-defined known-state for types of failures, preserving system state information in failure.	5	
CM0045	Error Detection and Correcting Memory	Use Error Detection and Correcting (EDAC) memory and integrate EDAC scheme with fault management and cyber-protection mechanisms to respond to the detection of uncorrectable multi-bit errors, other than time-delayed monitoring of EDAC telemetry by the mission operators on the ground. The spacecraft should utilize the EDAC scheme to routinely check for bit errors in the stored data on board the spacecraft, correct the single-bit errors, and identify the memory addresses of data with uncorrectable multi-bit errors of at least order two, if not higher order in some cases.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0046	Long Duration Testing	Perform testing using hardware or simulation/emulation where the test executes over a long period of time (30+ days). This testing will attempt to flesh out race conditions or time-based attacks.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0047	Operating System Security	Ensure spacecraft's operating system is scrutinized/whitelisted and has received adequate software assurance previously. The operating system should be analyzed for its attack surface and non-utilized features should be stripped from the operating system. Many real-time operating systems contain features that are not necessary for spacecraft operations and only increase the attack surface.	Functional	intersects with	Least Functionality	CFG-03	Mechanisms exist to configure systems to provide only essential capabilities by specifically prohibiting or restricting the use of ports, protocols, and/or services.	5	
			Functional	intersects with	Configure Systems, Components or Services for High-Risk Areas	CFG-02.5	Mechanisms exist to configure systems utilized in high-risk areas with more restrictive baseline configurations.	5	
			Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
			Functional	intersects with	System Hardening Through Baseline Configurations	CFG-02	Mechanisms exist to develop, document and maintain secure baseline configurations for technology platforms that are consistent with industry-accepted system hardening standards.	5	
CM0048	Resilient Position, Navigation, and Timing	If available, use an authentication mechanism that allows GNSS receivers to verify the authenticity of the GNSS information and of the entity transmitting it, to ensure that it comes from a trusted source. Have fault-tolerant authoritative time sourcing for the spacecraft's clock. The spacecraft should synchronize the internal system clocks for each processor to the authoritative time source when the time difference is greater than the FSW-defined interval. If Spacewire is utilized, then the spacecraft should adhere to mission-defined time synchronization standard/protocol to synchronize time across a Spacewire network with an accuracy around 1 microsecond.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0049	Machine Learning Data Integrity	When AI/ML is being used for mission critical operations, the integrity of the training data set is imperative. Data poisoning against the training data set can have detrimental effects on the functionality of the AI/ML. Fixing poisoned models is very difficult so model developers need to focus on countermeasures that could either block attack attempts or detect malicious inputs before the training cycle occurs. Regression testing over time, validity checking on data sets, manual analysis, as well as using statistical analysis to find potential injects can help detect anomalies.	Functional	intersects with	Data Source Integrity	AAT-12.2	Mechanisms exist to protect the integrity of source data to prevent accidental contamination or malicious corruption (e.g., data poisoning) that could compromise the performance of Artificial Intelligence and Autonomous Technologies (AAT).	5	
			Functional	intersects with	Data Source Identification	AAT-12.1	Mechanisms exist to identify and document data sources utilized in the training and/or operation of Artificial Intelligence and Autonomous Technologies (AAT).	5	
			Functional	intersects with	Provenance	AST-03.2	Mechanisms exist to track the origin, development, ownership, location and changes to systems, system components and associated data.	5	
CM0050	On-board Message Encryption	In addition to authentication on-board the spacecraft bus, encryption is also recommended to protect the confidentiality of the data traversing the bus.	Functional	intersects with	Use of Cryptographic Controls	CRY-01	Mechanisms exist to facilitate the implementation of cryptographic protections controls using known public standards and trusted cryptographic technologies.	5	
CM0051	Fault Injection Redundancy	To counter fault analysis attacks, it is recommended to use redundancy to catch injected faults. For certain critical functions that need protected against fault-based side channel attacks, it is recommended to deploy multiple implementations of the same function. Given an input, the spacecraft can process it using the various implementations and compare the outputs. A selection module could be incorporated to decide the valid output. Although sensor nodes have limited resources, critical regions usually comprise the crypto functions, which must be secured.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0052	Insider Threat Protection	Establish policy and procedures to prevent individuals (i.e., insiders) from masquerading as individuals with valid access to areas where commanding of the spacecraft is possible. Establish an Insider Threat Program to aid in the prevention of people with authorized access performing malicious activities.	Functional	intersects with	Insider Threat Program	THR-04	Mechanisms exist to implement an insider threat program that includes a cross-discipline insider threat incident handling team.	5	
			Functional	intersects with	Insider Threat Awareness	THR-05	Mechanisms exist to utilize security awareness training on recognizing and reporting potential indicators of insider threat.	5	
			Functional	intersects with	Insider Threat Response Capability	IRO-02.2	Mechanisms exist to implement and govern an insider threat program.	5	
			Functional	intersects with	Insider Threats	MON-16.1	Mechanisms exist to monitor internal personnel activity for potential security incidents.	5	
CM0053	Physical Security Controls	Employ physical security controls (badge with pins, guards, gates, etc.) to prevent unauthorized access to the systems that have the ability to command the spacecraft.	Functional	intersects with	Physical & Environmental Protections	PES-01	Mechanisms exist to facilitate the operation of physical and environmental protection controls.	5	
CM0054	Two-Person Rule	Utilize a two-person system to achieve a high level of security for systems with command level access to the spacecraft. Under this rule all access and actions require the presence of two authorized people at all times.	Functional	intersects with	Two-Person Rule	HRS-12.1	Mechanisms exist to enforce a two-person rule for implementing changes to sensitive systems.	5	
CM0055	Secure Command Mode(s)	Provide additional protection modes for commanding the spacecraft. These can be where the spacecraft will restrict command lock based on geographic location of ground stations, special operational modes within the flight software, or even temporal controls where the spacecraft will only accept commands during certain times.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CM0056	Data Backup	Implement disaster recovery plans that contain procedures for taking regular data backups that can be used to restore critical data. Ensure backups are stored off system and is protected from common methods adversaries may use to gain access and destroy the backups to prevent recovery.	Functional	intersects with	Data Backups	BCD-11	Mechanisms exist to create recurring backups of data, software and/or system images, as well as verify the integrity of these backups, to ensure the availability of the data to satisfying Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).	5	
CM0057	Tamper Resistant Body	Using a tamper resistant body can increase the one-time cost of the sensor node but will allow the node to conserve the power usage when compared with other countermeasures.	Functional	intersects with	Tamper Protection	AST-15	Mechanisms exist to verify logical configuration settings and the physical integrity of critical technology assets throughout their lifecycle.	5	
CM0058	Power Randomization	Power randomization is a technique in which a hardware module is built into the chip that adds noise to the power consumption. This countermeasure is simple and easy to implement but is not energy efficient and could be impactful for size, weight, and power which is limited on spacecraft as it adds to the fabrication cost of the device.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0059	Power Consumption Obfuscation	Design hardware circuits or perform obfuscation in general that mask the changes in power consumption to increase the cost/difficulty of a power analysis attack. This will increase the cost of manufacturing sensor nodes.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0060	Secret Shares	Use of secret shares in which the original computation is divided probabilistically such that the power subset of shares is statistically independent. One of the major drawbacks of this solution is the increase in the power consumption due to the number of operations that are almost doubled.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0061	Power Masking	Masking is a scheme in which the intermediate variable is not dependent on an easily accessible subset of secret key. This results in making it impossible to deduce the secret key with partial information gathered through electromagnetic leakage.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0062	Dummy Process - Aggregator Node	According to Securing Sensor Nodes Against Side Channel Attacks, it is practically inefficient to prevent adversaries from identifying aggregator nodes in a network (i.e., constellation) because camouflaging traffic in sensor networks is power intensive. Consequently, focus on preventing adversaries from identifying valid aggregation cycles of aggregator nodes. One solution to counter such attacks is to have each aggregator node execute dummy operations that resemble the average power consumption curve observed during the normal operation of the aggregator node. Apart from simulating the power consumption of a genuine process execution, the two necessities that the execution of the dummy process must incorporate to be successful in thwarting the accumulation phase are to use a different dummy execution process each time or have a low repetition rate. This should help prevent the attacker from finding a pattern that would differentiate the execution of a dummy process from the normal execution of an aggregator node. The second requirement relates to the timing of the execution of the dummy process. Depending on whether there is a pattern to the timing of the execution of a dummy process, a threat actor may be able to identify and disregard the dummy process. For example, if a threat actor is capable of identifying the presence or absence of a radio frequency transmission, the attacker can disregard any power consumption curve computed during the absence of transmission signal. Similarly, if the dummy process is not executed every time the aggregator node receives a transmission, the attacker will be able to identify invalid transmission. Hence, to ensure the effectiveness of this scheme, the dummy process must be executed each time the aggregator receives a transmission as well as randomly during idle periods. The advantage of incorporating dummy processes in an aggregator is to minimize the ease of identifying transmission flow in a sensor network that can be used to identify the base station of the sensor network, which could be highly confidential in critical applications.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0063	Increase Clock Cycles/Timing	Use more clock cycles such that branching does not affect the execution time. Also, the memory access times should be standardized to be the same over all accesses. If timing is not mission critical and time is in abundance, the access times can be reduced by adding sufficient delay to normalize the access times. These countermeasures will result in increased power consumption which may not be conducive for low size, weight, and power missions.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0064	Dual Layer Protection	Use a dual layered case with the inner layer a highly conducting surface and the outer layer made of a non-conducting material. When heat is generated from internal computing components, the inner, highly conducting surface will quickly dissipate the heat around. The outer layer prevents accesses to the temporary hot spots formed on the inner layer.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0065	OSAM Dual Authorization	Before engaging in an On-orbit Servicing, Assembly, and Manufacturing (OSAM) mission, verification of servicer should be multi-factor authenticated/authorized by both the serviced ground station and the serviced asset.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0066	Model-based System Verification	Real-time physics model-based system verification of state could help to verify data input and control sequence changes	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0067	Smart Contracts	Smart contracts can be used to mitigate harm when an attacker is attempting to compromise a hosted payload. Smart contracts will stipulate security protocol required across a bus and should it be violated, the violator will be barred from exchanges across the system after consensus achieved across the network.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0068	Reinforcement Learning	Institute a reinforcement learning agent that will detect anomalous events and redirect processes to proceed by ignoring malicious data/input.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0069	Process White Listing	Simple process ID whitelisting on the firmware level could impede attackers from instigating unnecessary processes which could impact the spacecraft	Functional	intersects with	Explicitly Allow / Deny Applications	CFG-03.3	Mechanisms exist to explicitly allow (allowlist / whitelist) and/or block (denylist / blacklist) applications that are authorized to execute on systems.	5	
CM0070	Alternate Communications Paths	Establish alternate communications paths to reduce the risk of all communications paths being affected by the same incident.	Functional	intersects with	Alternate Communications Paths	BCD-10.4	Mechanisms exist to maintain command and control capabilities via alternate communications channels and designating alternative decision makers if primary decision makers are unavailable.	5	
CM0071	Communication Physical Medium	Establish alternate physical medium for networking based on threat model/environment. For example, fiber optic cabling is commonly perceived as a better choice in lieu of copper for mitigating network security concerns (i.e., eavesdropping / traffic flow analysis) and this is because optical connections transmit data using light, they don't radiate signals that can be intercepted.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0072	Protocol Update / Refactoring	A protocol is a set of rules (i.e., formats and procedures) to implement and control some type of association (e.g., communication) between systems. Protocols can have vulnerabilities within their specification and may require updating or refactoring based on vulnerabilities or emerging threats (i.e., quantum computing).	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0073	Traffic Flow Analysis Defense	Utilizing techniques to assure traffic flow security and confidentiality to mitigate or defeat traffic analysis attacks or reduce the value of any indicators or adversary inferences. This may be a subset of COMSEC protections, but the techniques would be applied where required to links that carry TT&C and/or data transmissions (to include on-board the spacecraft) where applicable given value and attacker capability. Techniques may include but are not limited to methods to pad or otherwise obfuscate traffic volumes/duration and/or periodicity, concealment of routing information and/or endpoints, or methods to frustrate statistical analysis.	Functional	intersects with	Inbound & Outbound Communications Traffic	MON-01.3	Mechanisms exist to continuously monitor inbound and outbound communications traffic for unusual or unauthorized activities or conditions.	5	
			Functional	intersects with	Network Intrusion Detection / Prevention Systems (NIDS / NIPS)	NET-08	Mechanisms exist to employ Network Intrusion Detection / Prevention Systems (NIDS/NIPS) to detect and/or prevent intrusions into the network.	5	
			Functional	intersects with	Analyze Traffic for Covert Exfiltration	MON-11.1	Automated mechanisms exist to analyze network traffic to detect covert data exfiltration.	5	
CM0074	Distributed Constellations	A distributed system uses a number of nodes, working together, to perform the same mission or functions as a single node. In a distributed constellation, the end user is not dependent on any single satellite but rather uses multiple satellites to derive a capability. A distributed constellation can complicate an adversary's counterspace planning by presenting a larger number of targets that must be successfully attacked to achieve the same effects as targeting just one or two satellites in a less-distributed architecture. GPS is an example of a distributed constellation because the functioning of the system is not dependent on any single satellite or ground station; a user can use any four satellites within view to get a time and position fix.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	intersects with	Distributed Processing & Storage	SEA-15	Mechanisms exist to distribute processing and storage across multiple physical locations.	5	
CM0075	Proliferated Constellations	Proliferated satellite constellations deploy a larger number of the same types of satellites to similar orbits to perform the same missions. While distribution relies on placing more satellites or payloads on orbit that work together to provide a complete capability, proliferation is simply building more systems (or maintaining more on-orbit spares) to increase the constellation size and overall capacity. Proliferation can be an expensive option if the systems being proliferated are individually expensive, although highly proliferated systems may reduce unit costs in production from the learning curve effect and economies of scale.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0076	Diversified Architectures	In a diversified architecture, multiple systems contribute to the same mission using platforms and payloads that may be operating in different orbits or in different domains. For example, wideband communications to fixed and mobile users can be provided by the military's WGS system, commercial SATCOM systems, airborne communication nodes, or terrestrial networks. The Chinese BeiDou system for positioning, navigation, and timing uses a diverse set of orbits, with satellites in geostationary orbit (GEO), highly inclined GEO, and medium Earth orbit (MEO). Diversification reduces the incentive for an adversary to attack any one of these systems because the impact on the overall mission will be muted since systems in other orbits or domains can be used to compensate for losses. Moreover, attacking space systems in diversified orbits may require different capabilities for each orbital regime, and the collateral damage from such attacks, such as orbital debris, could have a much broader impact politically and economically.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CM0077	Space Domain Awareness	The credibility and effectiveness of many other types of defenses are enabled or enhanced by the ability to quickly detect, characterize, and attribute attacks against space systems. Space domain awareness (SDA) includes identifying and tracking space objects, predicting where objects will be in the future, monitoring the space environment and space weather, and characterizing the capabilities of space objects and how they are being used. Exquisite SDA—information that is more timely, precise, and comprehensive than what is publicly available—can help distinguish between accidental and intentional actions in space. SDA systems include terrestrial-based optical, infrared, and radar systems as well as space-based sensors, such as the U.S. military's Geosynchronous Space Situational Awareness Program (GSSAP) inspector satellites. Many nations have SDA systems with various levels of capability, and an increasing number of private companies (and amateur space trackers) are developing their own space surveillance systems, making the space environment more transparent to all users.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0078	Space-Based Radio Frequency Mapping	Space-based RF mapping is the ability to monitor and analyze the RF environment that affects space systems both in space and on Earth. Similar to exquisite SDA, space-based RF mapping provides space operators with a more complete picture of the space environment, the ability to quickly distinguish between intentional and unintentional interference, and the ability to detect and geolocate electronic attacks. RF mapping can allow operators to better characterize jamming and spoofing attacks from Earth or from other satellites so that other defenses can be more effectively employed.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0079	Maneuverability	Satellite maneuver is an operational tactic that can be used by satellites fitted with chemical thrusters to avoid kinetic and some directed energy ASAT weapons. For unguided projectiles, a satellite can be commanded to move out of their trajectory to avoid impact. If the threat is a guided projectile, like most direct-ascent ASAT and co-orbital ASAT weapons, maneuver becomes more difficult and is only likely to be effective if the satellite can move beyond the view of the onboard sensors on the guided warhead.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0080	Stealth Technology	Space systems can be operated and designed in ways that make them difficult to detect and track. Similar to platforms in other domains, stealthy satellites can use a smaller size, radar-absorbing coatings, radar-deflecting shapes, radar jamming and spoofing, unexpected or optimized maneuvers, and careful control of reflected radar, optical, and infrared energy to make themselves more difficult to detect and track. For example, academic research has shown that routine spacecraft maneuvers can be optimized to avoid detection by known sensors.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0081	Defensive Jamming and Spoofing	A jammer or spoofer can be used to disrupt sensors on an incoming kinetic ASAT weapon so that it cannot steer itself effectively in the terminal phase of flight. When used in conjunction with maneuver, this could allow a satellite to effectively "dodge" a kinetic attack. Similar systems could also be used to deceive SDA sensors by altering the reflected radar signal to change the location, velocity, and number of satellites detected, much like digital radio frequency memory (DRFM) jammers used on many military aircraft today. A spacebased jammer can also be used to disrupt an adversary's ability to communicate.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQGGate with an ASAT weapon.	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0082	Deception and Decoys	Deception can be used to conceal or mislead others on the "location, capability, operational status, mission type, and/or robustness" of a satellite. Public messaging, such as launch announcements, can limit information or actively spread disinformation about the capabilities of a satellite, and satellites can be operated in ways that conceal some of their capabilities. Another form of deception could be changing the capabilities or payloads on satellites while in orbit. Satellites with swappable payload modules could have on-orbit servicing vehicles that periodically move payloads from one satellite to another, further complicating the targeting calculus for an adversary because they may not be sure which type of payload is currently on which satellite. Satellites can also use tactical decoys to confuse the sensors on ASAT weapons and SDA systems. A satellite decoy can consist of an inflatable device designed to mimic the size and radar signature of a satellite, and multiple decoys can be stored on the satellite for deployment when needed. Electromagnetic decoys can also be used in space that mimic the RF signature of a satellite, similar to aircraft that use airborne decoys, such as the ADM-160 Miniature Air-launched Decoy (MALD).* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0083	Antenna Nulling and Adaptive Filtering	Satellites can be designed with antennas that "null" or minimize signals from a particular geographic region on the surface of the Earth or locations in space where jamming is detected. Nulling is useful when jamming is from a limited number of detectable locations, but one of the downsides is that it can also block transmissions from friendly users that fall within the nulled area. If a jammer is sufficiently close to friendly forces, the nulling antenna may not be able to block the jammer without also blocking legitimate users. Adaptive filtering, in contrast, is used to block specific frequency bands regardless of where these transmissions originate. Adaptive filtering is useful when jamming is consistently within a particular range of frequencies because these frequencies can be filtered out of the signal received on the satellite while transmissions can continue around them. However, a wideband jammer could interfere with a large enough portion of the spectrum being used that filtering out the jammed frequencies would degrade overall system performance. * *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0084	Physical Seizure	A space vehicle capable of docking with, manipulating, or maneuvering other satellites or pieces of debris can be used to thwart spacebased attacks or mitigate the effects after an attack has occurred. Such a system could be used to physically seize a threatening satellite that is being used to attack or endanger other satellites or to capture a satellite that has been disabled or hijacked for nefarious purposes. Such a system could also be used to collect and dispose of harmful orbital debris resulting from an attack. A key limitation of a physical seizure system is that each satellite would be time- and propellant-limited depending on the orbit in which it is stored. A system stored in GEO, for example, would not be well positioned to capture an object in LEO because of the amount of propellant required to maneuver into position. Physical seizure satellites may need to be stored on Earth and deployed once they are needed to a specific orbit to counter a specific threat.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0085	Electromagnetic Shielding	Satellite components can be vulnerable to the effects of background radiation in the space environment and deliberate attacks from HPM and electromagnetic pulse weapons. The effects can include data corruption on memory chips, processor resets, and short circuits that permanently damage components.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0086	Filtering and Shuttering	Filters and shutters can be used on remote sensing satellites to protect sensors from laser dazzling and blinding. Filters can protect sensors by only allowing light of certain wavelengths to reach the sensors. Filters are not very effective against lasers operating at the same wavelengths of light the sensors are designed to detect because a filter that blocks these wavelengths would also block the sensor from its intended mission. A shutter acts by quickly blocking or diverting all light to a sensor once an anomaly is detected or a threshold is reached, which can limit damage but also temporarily interrupts the collection of data.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	
CM0087	Defensive Dazzling/Blinding	Laser systems can be used to dazzle or blind the optical or infrared sensors on an incoming ASAT weapon in the terminal phase of flight. This is similar to the laser infrared countermeasures used on aircraft to defeat heat-seeking missiles. Blinding an ASAT weapon's guidance system and then maneuvering to a new position (if necessary) could allow a satellite to effectively "dodge" a kinetic attack. It could also be used to dazzle or blind the optical sensors on inspector satellites to prevent them from imaging a satellite that wants to keep its capabilities concealed or to frustrate adversary SDA efforts.* *https://csis-website-prod.s3.amazonaws.com/s3fs-public/publication/210225_Harrison_Defense_Space.pdf?N2KWelzCz3hE3AaUUptSGMprDtBlBSQG	Functional	no relationship	N/A	N/A	No applicable SCF control	N/A	

FDE #	FDE Name	Focal Document Element (FDE) Description	STRM Rationale	STRM Relationship	SCF Control	SCF #	Secure Controls Framework (SCF) Control Description	Strength of Relationship (optional)	Notes (optional)
CM0088	Organizational Policy	Documenting cyber security policies is crucial for several reasons, paramount among them being the establishment of a clear, consistent framework for managing and protecting an organization's information assets. Such documentation serves as a foundational guideline that outlines the principles, procedures, and responsibilities that govern the security of information. Having well-documented security policies ensures that everyone in the organization, from the top management to the newest employee, is on the same page regarding security expectations and behaviors. It provides a reference point for all staff, helping them understand their roles and responsibilities in safeguarding sensitive data. By clearly defining what is expected, employees are better equipped to follow best practices and avoid actions that could compromise security. These policies act as a guide for implementing technical controls and security measures. They inform the selection, development, and maintenance of security tools and protocols, ensuring that there is a methodical approach to securing the organization's digital assets. In the event of a security incident, having a documented policy in place provides a roadmap for response and recovery, reducing the time and resources spent in mitigating the issue. As cybersecurity in space is an area where regulatory compliance is becoming increasingly stringent, having documented information security policies is often a legal or regulatory requirement, and not simply a best practice.	Functional	subset of	Publishing Cybersecurity & Data Protection Documentation	GOV-02	Mechanisms exist to establish, maintain and disseminate cybersecurity & data protection policies, standards and procedures.	10	
CM0089	Assessment & Authorization	The A&A process establishes the extent to which a particular design and implementation, meet a set of specified security requirements defined by the organization, government guidelines, and federal mandates into a formal authorization package.	Functional	intersects with	Information Assurance (IA) Operations	IAO-01	Mechanisms exist to facilitate the implementation of cybersecurity & data privacy assessment and authorization controls.	5	
CM0090	Continuous Monitoring	Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.	Functional	intersects with	Continuous Monitoring	MON-01	Mechanisms exist to facilitate the implementation of enterprise-wide monitoring controls.	5	