Space Systems Security and Resilience Landscape:

Zero Trust in the Space Environment

Publication: April 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

I. INTRODUCTION

In February 2021, the Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) created the Space Systems Critical Infrastructure Working Group (SSCIWG). The working group is a public-private, cross-sector body organized and co-chaired by government and industry partners to assess and manage risks associated with space systems security and resiliency. This working group will serve as the primary mechanism to collaborate and coordinate on strategies and policies to increase or enhance space system security and resiliency. It will identify and offer solutions to identified gaps among current government and private sector efforts to address space asset infrastructure risks. The working group will strive to inform and make recommendations to private sector owners and operators of critical infrastructure; federal departments and agencies; and state, local, tribal, and territorial governments on actionable, economically feasible, scalable, risk-based recommendations and best practices.

The SSCIWG was created in compliance with the Critical Infrastructure Partnership Advisory Council (CIPAC) to enable the members to deliberate and achieve consensus advice to the federal government. The SSCIWG has several subgroups, including one that focuses on Space Systems Security and Resilience Landscape. Over the past year, the subgroup has been drafting a white paper on Space Systems and Zero Trust Architecture (ZTA). The findings of this white paper, found below, represent the thoughts and recommendations developed by public and private sector members of the SSCIWG.

In the early days of space travel, space programs were seen as a sign of national prestige and governments monopolized the sector to retain geopolitical and military power.[1] However, the model of government-directed human space activity born in the 1960s has recently transformed to a new model dominated by the private sector. Commercial activity in space has increased exponentially in the last 15 years growing from $110 billion in 2005 to nearly $357 billion in 2020.[2] With large private investments in popularizing space, it should come as no surprise that satellites, spacecraft, and their ground-based infrastructure have quickly become a part of our daily lives. According to the Harvard Business Review, "In 2019, 95% of the estimated $366 billion in revenue earned in the space sector was from the *space-for-earth* economy: that is, goods or services produced in space for use on earth."[3] These space systems help enable essential services such as telecommunications and internet infrastructure and services, healthcare, transportation, energy, and financial systems.

II. PURPOSE

In January 2022, the Office of Management and Budget released the *Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture*.[4] Prior to this, the National Institute of Standards and Technology (NIST) developed guides to enhance cybersecurity across the space sector, including the foundational elements of Position, Navigation, and Timing (PNT),[5] space, link, ground, and user segments. The NIST Cybersecurity Framework (CSF) applies across space infrastructure as the CSF is a foundational element

[1] Weinzierl, M. and Sarang, M., "The Commercial Space Age is Here." *Harvard Business Review*, February 12, 2021, https://hbr.org/2021/02/the-commercial-space-age-is-here. Accessed on July 3, 2023.

[2] Ben-Itzhak, S., "Companies are Commercializing Outer Space. Do Government Programs Still Matter?" *The Washington Post*, January 11, 2022, https://www.washingtonpost.com/politics/2022/01/11/companies-are-commercializing-outer-space-do-government-programs-still-matter/. Accessed on July 3, 2023.

[3] Weinzierl, M. and Sarang, M., "The Commercial Space Age is Here." *Harvard Business Review*, February 12, 2021, https://hbr.org/2021/02/the-commercial-space-age-is-here. Accessed on July 3, 2023.

[4] "Office of Management and Budget Releases Federal Strategy to Move the U.S. Government Towards a Zero Trust Architecture." *The White House*, January 26, 2022, https://www.whitehouse.gov/omb/briefing-room/2022/01/26/office-of-management-and-budget-releases-federal-strategy-to-move-the-u-s-government-towards-a-zero-trust-architecture/. Accessed on July 3, 2023.

[5] "Position, Navigation, and Timing." *NIST Computer Security Resource Center*, August 21, 2020, https://csrc.nist.gov/Topics/Applications/positioning-navigation-timing. Accessed on July 3, 2023.

of modern cybersecurity across the U.S. government.[6] This strategy moves the U.S. government toward a "zero trust" approach to cybersecurity and represents a step forward in executing *Executive Order 14028 (EO 14028): Improving the Nation's Cybersecurity*. In concert, CISA released the Zero Trust Maturity Model which provides references for federal agencies transitioning toward a zero trust architecture.[7] Both the framework and the maturity model are foundational elements of the U.S. government's approach to implementing zero trust. The purpose of this report is to analyze and define opportunities for applying zero trust tenants across space infrastructure. This guide relies on components of the framework and seeks to analyze where and how they can be applied across the space infrastructure.

A. FOUNDATIONAL CYBERSECURITY PRINCIPLES

While this report primarily focuses on zero trust concepts, it is important to understand some basic cybersecurity principles first—Secure by Design (SBD), Secure by Default, and Cybersecurity Performance Goals (CPGs). A product is considered Secure by Design "when the security of the customers is a core business requirement, not just a technical feature. Secure by Design principles should be implemented during the design phase of a product's development lifecycle to dramatically reduce the number of exploitable flaws before they are introduced to the market for broad use or consumption."[8] This encourages technology manufacturers to take ownership at the highest level in protection their consumers and putting their safety first. There is also the concept of Secure by Default, where these products are considered secure right out of the box, and need little to no end user configuration or additional costs to control any access to their sensitive information.

Cybersecurity Performance Goals (CPGs) are defined as "a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people."[9] These CPGs are organized to align with the National Institute of Standards and Technology's (NIST) Cybersecurity Framework functions to Identify, Protect, Detect, Respond, and Recover in the event of a cybersecurity event. These CPGs are considered voluntary, and are aimed to assist small- and medium-sized organizations bolster their cybersecurity efforts in a way tailored to have the most impact with limited resources. The principles of Secure by Design and Cybersecurity Performance Goals should be foundational for developers and manufacturers to consider as they build these technologies that impact space systems, or any systems, in any meaningful way.

III. ZERO TRUST DEFINED

A. BACKGROUND

While zero trust concepts have been around for well over a decade, there is no consensus on what constitutes something as zero trust. As proof of this assertion, consider the following sources, definitions, and concepts of zero trust:

[6] "Cybersecurity Framework." *National Institute of Standards and Technology*, https://www.nist.gov/cyberframework. Accessed on July 3, 2023.

[7] "Zero Trust Maturity Model." *CISA*,https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model https://www.cisa.gov/zero-trust-maturity-model. Accessed on July 3, 2023.

[8] "Secure by Design." *CISA*, https://www.cisa.gov/securebydesignhttps://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model. Accessed on January 26, 2024.

[9] "Cross-Sector Cybersecurity Performance Goals." *CISA*, https://www.cisa.gov/cross-sector-cybersecurity-performance-goals. Accessed on January 26, 2024.

- Amazon[10]
- American Council for Technology-Industry Advisory Council (ACT-IAC)[11]
- CISA Zero Trust Maturity Model[12]
- DoD CIO[13]
- Forrester[14]
- Google BeyondCorp[15]
- Microsoft[16]
- NIST SP 800-207[17]
- National Security Agency[18]
- The Open Group[19]
- UK National Cybersecurity Center[20]
- and others[21]

While there are a multitude of descriptions, the working group describes the essence of zero trust as this:

> “Regardless of your network location I have zero trust in who you are, the device you are using, and your authorization to access the resource you want! I need to verify you, your device, and your authorization first before I can trust you and grant access to the resource you want.”

The continuous verification process is one of the key aspects of the zero trust approach. The NIST blog *Zero Trust Cybersecurity: ‘Never Trust Always Verify’* states that, “Every access request to a resource must be thoroughly evaluated dynamically and in real time based on access policies in place and current state of credentials, device, application and service, as well as other observable behavior and environmental attributes, before access may be granted.”[22]

[10] “What is Zero Trust on AWS?” *Amazon*, https://aws.amazon.com/security/zero-trust/. Accessed on July 3, 2023.
[11] “Zero Trust Cybersecurity Current Trends.” *American Council for Technology and Industry Advisory Council (ACT-IAC)*, https://www.actiac.org/documents/zero-trust-cybersecurity-current-trends. Accessed on July 3, 2023.
[12] “Zero-Trust Maturity Model.” *CISA*, https://www.cisa.gov/zero-trust-maturity-model. Accessed on July 3, 2023.
[13] “Department of Defense Releases Zero Trust Strategy and Roadmap.” *U.S. Department of Defense, DoD CIO*, https://www.defense.gov/News/Releases/Release/Article/3225919/department-of-defense-releases-zero-trust-strategy-and-roadmap/. Accessed on July 31, 2023.
[14] Holmes, D., Burn, J., “The Definition of Modern Zero Trust.” *Forrester*, January 24, 2022, https://www.forrester.com/blogs/the-definition-of-modern-zero-trust/. Accessed on July 3, 2023.
[15] “BeyondCorp.” *Google Cloud*, https://cloud.google.com/beyondcorp. Accessed on July 3, 2023.
[16] “Implementing a Zero Trust security model at Microsoft.” *Microsoft*, June 23, 2023, https://www.microsoft.com/en-us/insidetrack/implementing-a-zero-trust-security-model-at-microsoft. Accessed on July 3, 2023.
[17] “NIST Special Publication 800-207: Zero Trust Architecture.” *NIST Computer Security Resource Center*, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final. Accessed on July 3, 2023.
[18] “Embracing a Zero Trust Security Model.” *National Security Agency*, February 2021, https://media.defense.gov/2021/Feb/25/2002588479/-1/-1/0/CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF. Accessed on July 3, 2023.
[19] “Zero Trust.” *The Open Group*, https://www.opengroup.org/forum/security/zerotrust. Accessed on July 3, 2023.
[20] “Zero Trust Architecture Design Principles.” *National Cyber Security Centre*, July 23, 2021, https://www.ncsc.gov.uk/collection/zero-trust-architecture. Accessed on July 3, 2023.
[21] N. F. Syed, S. W. Shah, A. Shaghaghi, A. Anwar, Z. Baig and R. Doss, "Zero Trust Architecture (ZTA): A Comprehensive Survey," in *IEEE Access*, vol. 10, pp. 57143-57179, 2022, doi: 10.1109/ACCESS.2022.3174679.
[22] Kerman, A.,“Zero Trust Cybersecurity: ‘Never Trust, Always Verify.’” *NIST: Taking Measure*, October 28, 2020, https://www.nist.gov/blogs/taking-measure/zero-trust-cybersecurity-never-trust-always-verify. Accessed on July 3, 2023.

IV. NIST ZERO TRUST TENETS

NIST, "…develops cybersecurity standards, guidelines, best practices, and other resources to meet the needs of U.S. industry, federal agencies, and the broader public."[23] In the U.S. government and industry, NIST's guidance (e.g., NIST SP 800-53) forms a baseline and therefore stands out as being particularly pertinent as an example. In NIST Special Publication 800-207, they define seven zero trust tenets. In abbreviated format, they are:

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-session basis.
4. Access to resources is determined by dynamic policy—including the observable state of client identity, application/service, and the requesting asset—and may include other behavioral and environmental attributes.
5. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
6. All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
7. The enterprise collects as much information as possible about the current state of assets, network infrastructure and communications and uses it to improve its security posture.[24]

In *Table 1* below, the data and computing services are resources that are refined into types, allowing fine-grained access control. Once an entity is authorized (and that entity can be a person, or a non-person such as an artificial intelligence agent or another software process), the communications are secured. One way to secure communications is via encryption or segmentation. The access to individual enterprise resources is done on a continuing basis, per session.

Because credentials are compromised often by threat actors (see MITRE ATT&CK[25] for more details), the zero trust tenets make it harder for a single compromise to spread across the network. The devices must first pass a health check (e.g., which device, patch levels, etc.) before being further considered for resource access. Dynamic policy allows access decisions to factor in a great deal of information on users, systems, and devices when considering access (e.g., time of day, user location, user role, simultaneous logins from vastly different network locations, anomalous behavior, etc.). The principle of least privilege is enforced, which can assist in reducing a common threat actor technique of privilege escalation. A multitude of sensors are arranged and traffic tapped, and automation is deployed to flag and react with protective measures that limit the damage of an attack.

[23] "Cybersecurity." *National Institute of Standards and Technology*, https://www.nist.gov/cybersecurity. Accessed on July 3, 2023.
[24] Rose, S., Borchert, O., Mitchell, S., Connelly, S., "NIST Special Publication 800-27: Zero Trust Architecture." *NIST Computer Security Resource Center,* August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final. Accessed on July 3, 2023.
[25] "MITRE ATT&CK." *The MITRE Corporation*, https://attack.mitre.org/. Accessed on July 3, 2023.

Table 1: Common Zero Trust Concepts[26]

Concept	Description
Just in Time Access	Involves authentication and access decisions based on a policy decision made at the time of the access request.
Just Enough Access	Ensures that only those privileges needed to carry out the request are provided for the duration of the request.
Tokenization or Encryption of Data	Ensures sensitive data becomes non-sensitive (for instance, by replacing a name with an arbitrary identifier) the data-attack surface is reduced because there are no sensitive data to access.
Dynamic Access Control Policies	Access control policies must be dynamic and computed from as many sources of data as possible.

V. FIVE KEY IMPLEMENTATION NEEDS OF ZERO TRUST IN MORE DETAIL

In this section, the working group compared the four leading federal government guidance documents pertaining to zero trust and binned their recommendations into a grouping of five key elements to create zero trust access control: Universal Authentication, Policy-Based Access Controls (Principle of Least Privilege), Network Segmentation (Principle of Least Access), Ubiquitous Encryption (e.g., secure communication), and Continuous Monitoring and Adjustment. The details are found in each of the documents, but the following table highlights some major commonalities within these five groupings.

Figure 1: Five ZTA Implementation Needs Interpreted within Four Documents

ZTA Implementation Needs	OMB M-22-09 (26 Jan 22)	CISA ZTMM 1.0 ** (Sep 21)	DoD ZT Ref Arch V2.0 (Jul 22)	NIST SP800-207 (Aug 20)
Universal Authentication • *Unique Identification of Users/Devices*	Federal staff have enterprise-managed accounts • *Strong MFA, enforced at apps* • *Complete Inventory of Every Device* • *Centralized Id Mgmt Sys, SSO*	P1: Identify – M2: Advanced – MFA, some federation of systems to M3: Optimal – Continuous validation P2: Device – M1: Trad'l – Some inventory	P1: User – MFA and continuous MFA, AuthN P2: Device – ability to identify device and device compliance, AuthN	T1: All data sources and computing services are considered resources
Policy-Based Access Controls (Principle of Least Privilege) • *Non-bypassable* • *Default Deny* • *Least Privilege* • *Role Based Access Cntl* • *Attribute-Based Access Cntl*	Federal security teams and data teams develop data categories and security rules to automatically detect and ultimately block unauthorized access to sensitive information.	P4: Application – M2: Advanced – Access based on centralize AuthN to M3: Optimal – Access is continually AuthZ P5: Data – M2: Advanced – Least Privilege access control	P1: User – RBAC and ABAC, Privilege Access Mgmt P2: Device – AuthZ P3: Network/Env – Manage Privileged access	T4: Access to resources is determined by dynamic policy T6: All resource authentication and authorization are dynamic and strictly enforced before access is allowed
Network Segmentation (Principle of Least Access)	Agency systems are isolated from each other • *User should log into applications, not networks*	P3: Network – M2: Advanced – Defined by ingress/egress micro-perimeters to M3: Optimal – Fully distributed ingress/egress micro-perimeters	P3: Network/Env – Segment physically & logically, prevent lateral movement	T3: Access to individual enterprise resources is granted on a per-session basis

[26] Shore, M., Zeadally, S., and Leshariya, A., "Zero Trust: The What, How, Why, and When," *Computer*, vol. 54, no. 11, pp. 26-25, November 2021, doi: 10.1109/MC.2021.3090018.

ZTA Implementation Needs	OMB M-22-09 (26 Jan 22)	CISA ZTMM 1.0 ** (Sep 21)	DoD ZT Ref Arch V2.0 (Jul 22)	NIST SP800-207 (Aug 20)
Ubiquitous Encryption	Network traffic flowing between and within them is reliably encrypted • *Encrypt DNS and http traffic*	P3: Network – M3: Optimal – all traffic is encrypted P5: Data – M3: Optimal – all data is encrypted at rest	P5: Data – encrypt data at rest	T2: All communication is secured regardless of network location
Continuous Monitoring and Adjustment	Federal staff devices are consistently tracked and monitored device's security posture used for access decisions to resources • *Secure Application Dev* • *Prevent, Detect and Respond to incidents on devices (CDM & EDR)* • *Enterprise-wide logging, info sharing* • *External scans of infrastructure*	P2: Device – M2: Advanced – Compliance enforcement and access depends on security posture on first access to M3: Optimal – Constant Device Monitoring and access based on risk analytics	P2: Device – Real-time attestation/patching P4: Applications and Workload – DevSecOps P6: Visibility and Analytics – continuous monitoring, inspection of network traffic and apply unified analytics for data, applications, assets, and services P7: Automation and Orchestration – integrated with SIEM	T5: The enterprise monitors and measures the integrity and security posture of all owned and associated assets T7: The enterprise collects as much information as possible about the current state as assets, network infrastructure, and communications and uses it to improve its security posture

***Note: This white paper was developed prior to the April 2023 release of the CISA Zero Trust Maturity Model 2.0.*[27]

There is a great deal of logical overlap, although the terminology or exact technical security controls differ.

VI. U.S. FEDERAL GOVERNMENT TRANSITIONING TO ZERO TRUST

The Office of Management and Budget's memorandum titled *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* states the following: "In the current threat environment, the Federal Government can no longer depend on conventional perimeter-based defenses to protect critical systems and data. As President Biden stated in Executive Order (EO) 14028, 'Incremental improvements will not give us the security we need; instead, the Federal Government needs to make bold changes and significant investments in order to defend the vital institutions that underpin the American way of life.'"[28]

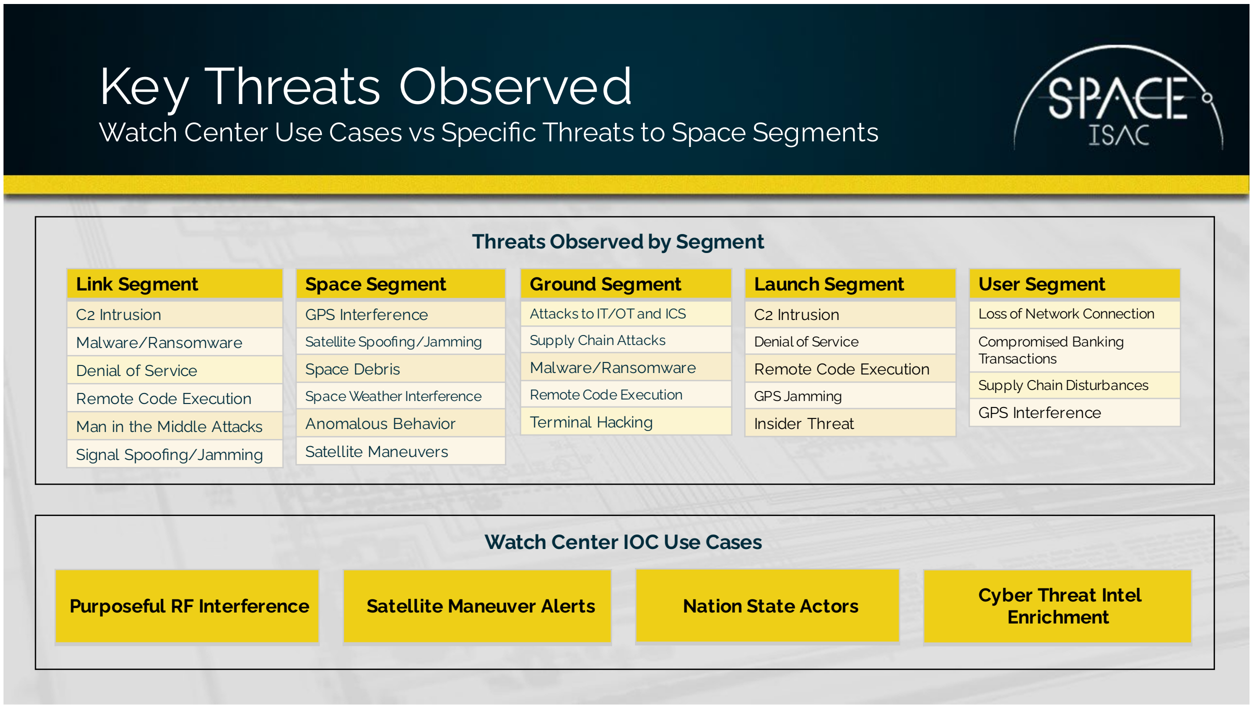
VII. SPACE INFORMATION SHARING AND ANALYSIS CENTER (ISAC)

The Space Information Sharing and Analysis Center (ISAC), "…serves to facilitate collaboration across the global space industry to enhance our ability to prepare for and respond to vulnerabilities, incidents, and threats; to disseminate timely and actionable information among member entities; and to serve as the primary communications channel for the sector with respect to this information."[29]

The Space ISAC is developing a watch center that can both take threat information that ISAC members provide and disseminate the information to the space community. *Figure 2: Space ISAC Key Threats Observed* illustrates the types of threats that are typically encountered by the space community.

[27] CISA Zero Trust Maturity Model 2.0, April 11, 2023, https://www.cisa.gov/resources-tools/resources/zero-trust-maturity-model. Accessed on July 3, 2023.
[28] Young, S. D., "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," *Executive Office of the President, Office of Management and Budget*, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf. Accessed on July 3, 2023.
[29] "Space ISAC," *Space Information Sharing and Analysis Center*. https://s-isac.org/. Accessed on July 3, 2023.

Figure 2: Space ISAC Key Threats Observed[30]



Key Threats Observed

Watch Center Use Cases vs Specific Threats to Space Segments

Threats Observed by Segment

Link Segment	Space Segment	Ground Segment	Launch Segment	User Segment
C2 Intrusion	GPS Interference	Attacks to IT/OT and ICS	C2 Intrusion	Loss of Network Connection
Malware/Ransomware	Satellite Spoofing/Jamming	Supply Chain Attacks	Denial of Service	Compromised Banking Transactions
Denial of Service	Space Debris	Malware/Ransomware	Remote Code Execution	Supply Chain Disturbances
Remote Code Execution	Space Weather Interference	Remote Code Execution	GPS Jamming	GPS Interference
Man in the Middle Attacks	Anomalous Behavior	Terminal Hacking	Insider Threat	
Signal Spoofing/Jamming	Satellite Maneuvers			

Watch Center IOC Use Cases

Purposeful RF Interference

Satellite Maneuver Alerts

Nation State Actors

Cyber Threat Intel Enrichment

VIII. THREATS AND MITIGATIONS

The Defense Intelligence Agency's *Challenges to Security in Space* also identifies key threats to space systems, including ground site attacks, orbital threats, directed energy weapons, denial and deception, electronic warfare, cyberattacks, kinetic energy weapons, and nuclear detonation.[31]

The Aerospace Corporation's Center for Space Policy and Strategy has provided best practices and advice for securing the space environment against cyberattacks. Their paper titled *Defending Spacecraft in the Cyber Domain,* "…focuses on principles (e.g., onboard intrusion detection and prevention systems, hardware/software supply chain, and onboard logging) that aim to provide decisionmakers, acquisition professionals, program managers, and system designers alike with considerations while acquiring and designing cyber-resilient spacecraft."[32]

[30] *Figure 2: Space ISAC Key Threats Observed* is Space ISAC proprietary information provided to CISA by Space ISAC SSIWG members for use in this report. Do not share without express written permission from Space ISAC.

[31] "Challenges to Security in Space." *Defense Intelligence Agency*, 2022, https://www.dia.mil/Portals/110/Documents/News/Military_Power_Publications/Challenges_Security_Space_2022.pdf. Accessed on July 3, 2023.

[32] Bailey, B., Speelman, R. J., Doshi, P. A., Cohen, N. C., and Wheeler, W. A., "Defending Spacecraft in the Cyber Domain." *The Aerospace Corporation, Center for Space Policy and Strategy,* November 2019, https://aerospace.org/sites/default/files/2019-11/Bailey_DefendingSpacecraft_11052019.pdf. Accessed on July 3, 2023.

IX. ZERO TRUST ROADMAP FOR SPACE SYSTEMS

The core components of any zero trust implementation are an organization's data, understanding how its data facilitates an organization's functions, and how access to this data is used to deliver its business or mission objectives. The organization labels and prioritizes data in functional contexts derived from business or mission objective requirements that necessitate access within established constraints (i.e., the right information, in the right place, and at the right time). This paper considers two starting points for implementing a zero trust architecture: existing systems and new acquisitions. The constraints are more prevalent when an organization with an existing system is driven to transition to a zero trust architecture while mitigating impacts this may have on operations. New acquisitions benefit from considering the data types, functions, and criticality early in conceptual development. In either case, each will continue to be challenged with integrating and sustainably using available technology to create a zero trust access control.

A mature and collaborative systems engineering approach will be key to a successful zero trust implementation. There are multiple system life cycle depictions, but they generally share the essence established by the generic life cycle described in ISO/IEC/IEEE 15288:2015.[33] An existing architecture or acquisition would benefit from systems engineering to define the roadmap to zero trust access control. The zero trust architecture for an existing system will need to work with constraints such as the availability of on-board processing cycles and memory to implement the ZTA functions. New acquisitions include these same constraints but also add to size, weight, and power limitations if considering additional hardware to implement a zero trust architecture.

To manage the constraints, the first step in the zero trust concept would emphasize scoping the implementation to the mission or business critical threads to create an architecture that is scalable to the operational needs for the mission (i.e., it must enable the required access for the number of users to the number of resources for the mission). The scalability requirements need the essential threads supported by existing architecture to transition to a zero trust implementation as resources become available in iterative phases. *Table 3* depicts a generic roadmap with key activities and objectives toward implementing a zero trust architecture in the space domain.

Table 3: Roadmap Activities for Zero Trust Architecture

Life Cycle Activity	Roadmap Objectives
Concept Development	• Identify mission essential functions for the following: 1. Space vehicle (SV) to SV 2. SV to ground (including control centers and users) 3. Ground to SV, and 4. Ground • Map the ZTA assets that support the mission essential functions (i.e., inventory data assets, components, internal, and external interfaces for each SV, ground station, and interconnections with product consumers) • Identify level of resources access control required (i.e., network level, application level, data level, etc.) for each mission essential function
Design and Development	• Develop the Least Access (i.e., Network Segmentation) architecture needed to limit lateral movement of an unauthorized user

[33] "Systems and software engineering – System life cycle processes," *ISO/IEC/IEEE 15288:2015*, May 2015, https://www.iso.org/standard/63711.html. Accessed on July 3, 2023.

Life Cycle Activity	Roadmap Objectives
	○ Separate the Control Plane from the Data Plane ○ Determine how and where to use Policy Enforcement Points • Develop the Ubiquitous Encryption plans for securing the end-to-end ZTA sessions, including the key and certificate management plans • Perform initial ZTA requirements definitions and derivations (based on Figure 1) • Conduct trade studies of products needed to implement the ZTA requirements and alternative design options to accomplish: ○ Inventory collection, dynamic discovery, and workflow facilitation ○ Network wide encryption, segmentation, and modification workflow ○ Identity management, access control, and provisioning/deprovisioning workflow facilitation ○ Dynamic data, device, and identity state evaluation and revocation workflow ○ Decentralized decision and enforcement mechanism (extended to the space vehicle), and modification workflow ○ Telemetry collection, dynamic analysis, report, and decision workflow • Develop the training curriculum and delivery approach, maintenance manuals, and monitoring and incident response tools, tactics, and procedures
Test and Production	• Build as designed • Integrate, test, verify, and validate zero-trust elements perform as required
Operate and Support	• Constantly monitor, analyze, adjust, and enforce policies and processes • Use applicable threat intelligence and indicators of compromise to facilitate fine-tuning of ZTA policies
Retirement	• Retain to facilitate next generation ZTA development and implementation

X. CASE STUDIES

A. Operational Satellite Service Use Case

The space cyber architecture is also relevant for defense space projects or operations. The operational satellite service use case below demonstrates how the policy and enforcement approach would apply in an end-to-end defense environment. The use case describes how two different security zones in the strategic domain are both connected to an IP-enabled satellite ground station. The ground station is then providing connectivity to the tactical and deployed domains.

Each domain has its own security policy decision point, and a policy enforcement point to police traffic in and out of the domain (and traffic within the domain as well).

Focusing on the space segments, the satellite ground station is managing connections to its strategic terrestrial domains and to the satellite itself. Conceptually, a whole-of-defense strategic policy decision point sits outside the individual domains and provides high-level guidance to the individual policy decision points. It is envisioned that this provides the settings to the network cyber postures akin to the SAFEBASE model, a risk management and response tool that is applied to the defense bases. Just like the SAFEBASE model, each network will have unique responses to the high-level external guidance. This is the same as the response to the threat feeds provided as part of the standard architecture that come from the security industry and security vendors.

The satellite ground station has its own traffic policy decision point that considers the conditions of the traffic (i.e., user, device, location, application, etc.) and applies controls on the traffic to ensure that it is destined for assets in its own domain. Traffic that is passing through is not managed explicitly as it is most likely transparent to the ground station due to end-to-end encryption.

The satellite domain internal policy decision point is not likely to be subject to the policy settings of the high-level strategic policy or tactical strategic policy, primarily as it is a specialized environment managed via satellite operations centers, which themselves can take guidance from threat feeds and external policy settings. However, what is expected going forward is a greater level of autonomous threat detection and reaction onboard the satellite itself. The amount of autonomous threat detection and reaction is highly dependent on factors such as who is managing the satellite (internal or outsourced), what other hosted payloads are on the satellite (if any), and whether it is a commercial or military satellite. This is more likely in environments such as a low earth orbit (LEO) satellite when the device is out of reach of ground controllers for much of its lifetime.

Increasingly, satellites are being used in the tactical domain, not just for communications backhaul but for providing sensor services direct to soldiers in the field. In this domain, it is likely that in the future, the threat posture of systems in tactical or deployed environments will be self-determined. In isolation using and security policy, settings will be raised or lowered depending on the tempo of events, and the wider cybersecurity threat environment. An example of this is that a LEO satellite internal policy decision point considers its current location (and hence, location of its terrestrial connections) when making policy decisions on incoming connection requests.

If a change occurs in the tactical domain, and a new policy setting is issued from the tactical or deployed policy engine to the ground station, the next time the LEO satellite connects, it will receive the new policy settings and change its geo-blocking behaviors depending on the new ground situation in the tactical domain. While this situation may sound futuristic, there are many aspects of this already occurring today. What is missing is the end-to-end synchronization of these policies with the wider cyber posture of the environment.

B. Research and Development (R&D) IN ZTA

There are several emergent areas of zero trust architectures relevant to space systems. Three that are promising include the use of homomorphic encryption, distributed ledger technology, and quantum communication.

1. Homomorphic Encryption

Homomorphic encryption, defined by IBM as an "…innovative technology that can help you achieve zero trust by unlocking the value of data on untrusted domains without needing to decrypt it," offers a solution to computational outsourcing of sensitive or private information.[34] Homomorphism preserves the structure of data as the data is mapped to an output space. In the realm of information encryption, the mapped space represents the encrypted data. The homomorphic property of such structures allows a user to perform meaningful mathematical operations on the encrypted data, as the relationship among elements within the structure is preserved. After mathematical operations are completed, the decrypted result can be ascertained by mapping back to the original space. This offers a unique scheme for data processing, as it allows a user to

[34] "What is homomorphic encryption?" *IBM*, https://www.ibm.com/topics/homomorphic-encryption. Accessed on July 13, 2023.

share data with an external party, enables the external entity to operate on the data without decrypting or corrupting it, and returns the final result to the user who can decrypt it and reveal the true calculated value.[35] Such an architecture is highly beneficial to a user who lacks the processing resources to conduct secure and efficient computation with a third party. Today's ubiquitous use of cloud computing and data storage offers application opportunities for homomorphic encryption by allowing computation on encrypted data.

Homomorphic encryption schemes have been implemented, but their potential for space applications has not been explored because of their need for high-intensity processing which is not always possible in space weight and power (SWAP) constrained space systems. Other industries, such as healthcare, infrastructure, and energy, have implemented homomorphic encryption schemes to allow for remote processing and analysis of data (applications of homomorphic encryption). Similar approaches could be applied to space to create a ZTA. A promising example is the implementation of homomorphic encryption for controller purposes; a controller can compute on encrypted data rather than decrypting first, limiting key sharing and increasing efficiency and security (encrypting controller using fully homomorphic encryption for security of cyber-physical systems). Implementation of homomorphic encryption would help achieve the principle of least access by minimizing the access of third parties to decrypted data while still allowing for productive data sharing and analysis. Nevertheless, such encryption schemes have yet to be applied to space systems, and their technology readiness level remains low. A second technology that can help reach ZTA is distributed ledgers.

2. Distributed Ledger Technology

Distributed ledgers offer a new architecture for storing and validating data. The ledger contains published transactions that can be referred to when examining previous actions. The ledger is published to all users, allowing monitoring of actions by all parties. In the space of ZTA, distributed ledgers would help support continuous monitoring and allow malicious actors to be held accountable. In addition to visibility across a distributed network of owners and operators, distributed ledgers have been engaged for goods and services exchanged through smart contracts. Smart contracts can dictate terms of a transaction where the transaction can only be processed by hashing it to the ledger once there is consensus among the majority of nodes that the transaction is valid. Consensus-based distributed ledgers offer a means to achieve trustless transactions; hence the growth of cryptocurrencies such as bitcoin. Smart contracts that engage distributed ledgers can be applied for space applications to enable interaction between non-trustworthy parties for a variety of computational services; the Orbital Resilient Blockchain Interagent Transaction Service (ORBITS), sponsored by Defense Advanced Research Projects Agency (DARPA), is an example of applied distributed ledgers to improve confidence between a provider and client of space servicing. Development of distributed ledgers for space applications will need to overcome challenges that accompany the architecture, such as increased hardware complexity, computational overhead, and the fact that the security of the ledger varies with the number of users participating in it.

3. Quantum Communication Technology

Large leaps in quantum research have opened the door for the manipulation of quantum entanglement for information distribution and storage. Quantum communication could be accomplished through quantum key distribution, which would encode information in a single, entangled photon and allow for the sharing of quantum, secret keys. This could allow for heightened security through the creation of robust encryption in a ZTA system. Additionally, dedicated quantum links could help network segmentation by establishing

[35] Neela, K. L., and Kavitha, V., "A Survey on Security Issues and Vulnerabilities on Cloud Computing*." International Journal of Computer Science & Engineering Technology (IJCSET)*, vol 4, no. 7, pp. 855-860, Jul. 2013, doi: 10.1.1.403.6661.

nontraditional communication avenues.[36] This technology has been tested in the space environment, but its technology readiness level remains low. Obstacles to deploying this technology in the space environment include the fact that quantum systems operate on specialized equipment that is costly.[37] While such technologies are still in the R&D phases, they should be considered for the design of future space systems to enable encrypted links for ZTA networks.

[36] Rabie, P., "Quantum communication takes a major leap with satellite-based experiment." *Space.com*, August 21, 2020, https://www.space.com/quantum-communication-major-leap-satellite-experiment.html. Accessed on July 5, 2023.

[37] "Quantum Key Distribution (QKD) and Quantum Cryptography (QC)." *National Security Agency,* https://www.nsa.gov/Cybersecurity/Quantum-Key-Distribution-QKD-and-Quantum-Cryptography-QC/)/. Accessed on July 5, 2023.

APPENDIX A: WORKING GROUP MEMBERS

Member	Company/Agency
Raymond Boncek	Lockheed Martin Corporation
Donald De Arment	Cybersecurity and Infrastructure Security Agency
Elizabeth Eigner	Microsoft
Daniel Floreani	CyberOps
Joel Francis	Space Information Sharing and Analysis Center
Ronald Keen	Cybersecurity and Infrastructure Security Agency
Kimberly King	The Aerospace Corporation
David Logsdon	CompTIA
Erin Miller	Space Information Sharing and Analysis Center
Lydia Siramdane	Peraton
Chelsea Smethurst	Microsoft
Shaun Thomas	Lockheed Martin Corporation

APPENDIX B: EXISTING ZERO TRUST FRAMEWORKS

NIST SP 800-207
1. All enterprise systems are considered resources.
2. The enterprise ensures all owned systems are in their most secure state possible.
3. All communication is done in a secure manner end-to-end and regardless of network location.
4. Access to individual enterprise resources is granted on a per-connection basis.
5. User authentication is dynamic and strictly enforced before access.
6. Access to resources is determined by policy, including the observable continuous monitoring and adjustment of policy of user, system, and environment.
7. The enterprise monitors and measures the integrity and security posture of all owned and associated assets.

Zero Trust Reference Architecture
1. Assume a hostile environment
2. Presume breach
3. Never trust, always verify
4. Scrutinize explicitly
5. Apply unified analytics

CISA’s Five Zero Trust Pillars
1. Identify
2. Devices
3. Networks
4. Applications and Workloads
5. Data

APPENDIX C: FEDERAL AND INTERNATIONAL ZERO TRUST INITIATIVES AND ANALYSIS

Federal and International Zero Trust Initiatives
1. NIST Cybersecurity **and** Risk Management Framework/FISMA – Planning
2. FICAM – Identity Provisioning
3. OMB M-22-09 Moving the U.S. Government Toward Zero Trust Cybersecurity Principles[38]
4. CISA Continuous Diagnostics and Mitigation (CDM) Program – ID/Device/Application management
5. Smart Cloud and Data Center Optimization Initiative update (OMB M-19-19)
6. Trusted Internet Connections
7. National Security Agency "Applying Zero Trust to Defensive Monitoring for Space and Weapons Systems"

[38] Young, S. D., "Moving the U.S. Government Toward Zero Trust Cybersecurity Principles," *Executive Office of the President, Office of Management and Budget,* January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf. Accessed on July 5, 2023.

PRODUCT SURVEY

The Cybersecurity and Infrastructure Security Agency’s National Risk Management Center welcomes your feedback. Please complete the product survey at Space Systems Security and Resilience Landscape: Zero Trust in the Space Environment, or scan the QR code below: