INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-11 19:26 UTC

DHS S&T Advances Foundational Cybersecurity Research for Space Systems

GOVERNANCE | MEDIUM

SCC Item ID	SCC-GOV-2026-0051
Type	Governance
Severity	MEDIUM
Affected Products	Space systems, satellite infrastructure, ground station networks, critical infrastructure dependent on space-based services
Discovery Source	Gemini

Executive Summary

DHS Science and Technology Directorate is advancing foundational cybersecurity research for space systems, recognizing that satellite communications, GPS, and space-based timing infrastructure underpin power grids, financial networks, transportation, and other critical sectors. No standardized security framework exists dedicated to space system architectures, leaving ground segment interfaces, command-and-control links, and satellite supply chains without the mature regulatory guidance found in other critical infrastructure domains. Organizations dependent on space-based services for operational continuity face unquantified risk while baseline security metrics and resilience standards are still being developed.

Technical Analysis

This is a governance and research initiative item, not an active vulnerability disclosure. No CVE, CWE, or CVSS data applies. DHS S&T is conducting foundational research to establish security baselines for space system architectures, which currently lack dedicated standards. Key technical vulnerability domains identified in supporting sources include: ground segment interfaces (the primary attack surface for most demonstrated space system compromises), command-and-control link integrity (susceptibility to jamming, spoofing, and unauthorized command injection), supply chain integrity for satellite hardware and firmware components, and the absence of standardized authentication and encryption requirements for satellite-to-ground communications. Legislative proposals such as the Space Infrastructure Act seek formal designation of space systems as a 17th critical infrastructure sector under the National Infrastructure Protection Plan framework. CISA maintains an active risk management focus area for space systems. Confidence is medium, no specific DHS S&T announcement document was available for direct verification; supporting context is drawn from the CISA space systems page and CSC 2.0 reporting.

Action Checklist

1. Step 1: Inventory, catalog all operational dependencies on space-based services, including GPS timing for financial transaction sequencing, satellite communications for remote sites, and space-based positioning for logistics or operational technology environments (CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory).
2. Step 2: Detection, identify which internal systems consume GPS timing signals, satellite uplinks, or space-based data feeds; log any anomalies in timing drift, signal loss, or unexpected command-and-control behavior at ground station interfaces (NIST AU-2: Event Logging; NIST SI-4: System Monitoring).
3. Step 3: Assessment, review vendor security documentation for any space-based service providers in your supply chain and assess whether contractual security requirements address ground segment and link security (NIST SI-7: Software, Firmware, and Information Integrity).
4. Step 4: Recovery, establish resilience plans for degraded or denied space-based service scenarios; validate that backup timing, communications, and positioning sources exist for mission-critical operations dependent on GPS or satellite links (NIST IR-8: Incident Response Plan).
5. Step 5: Post-Incident, monitor CISA space systems risk management guidance and DHS S&T publications for emerging baseline standards; incorporate space system dependencies into your next risk assessment cycle and flag any third-party providers lacking documented space segment security controls (NIST IR-4: Incident Handling; CIS 7.1: Establish and Maintain a Vulnerability Management Process).

IR / Forensic Enrichment

Triage Priority	DEFERRED
Escalation Criteria	Escalate to immediate priority if active GPS timing anomalies (drift exceeding 100ms on stratum-1 servers), confirmed VSAT uplink interference, or a CISA emergency directive targeting space systems dependencies is issued; also escalate if a third-party space service provider discloses a breach affecting ground segment integrity or command-and-control link confidentiality.
Recovery Notes	Post-resilience-testing, verify that all NTP-dependent systems (financial transaction sequencers, OT PLCs, SCADA historians) have re-synchronized to GPS-disciplined stratum-1 sources and that no persistent timing offset exceeds the threshold defined in your operations baseline. Monitor GPS receiver lock status and C/N0 metrics continuously for 30 days following any signal anomaly to detect recurrence consistent with GPS spoofing or jamming campaigns. Update the space system dependency inventory and risk register to reflect any gaps discovered during tabletop or failover testing before closing the post-incident review cycle.

Forensic Artifacts	GPS receiver acquisition logs from stratum-1 NTP appliances (e.g., Spectracom SecureSync, Meinberg LANTIME): C/N0 degradation history, lock/unlock event timestamps, and almanac/ephemeris anomalies indicating spoofed satellite signals | NTP daemon logs ('chronyc tracking' history, ntpd drift file at /var/lib/ntp/ntp.drift) showing stratum changes, reference source substitutions, or frequency error spikes on systems dependent on GPS timing | Ground station modem and RF terminal logs: signal strength (Eb/N0), uplink power control adjustments, and any out-of-band management commands received on C2 interfaces (captured via Wireshark on ground station LAN segment) | Windows System Event Log Event ID 37 ('The time service has not been able to synchronize') and Event ID 29 ('The time service is now synchronizing') on Windows servers receiving NTP from GPS-disciplined sources, correlated with timestamps of any operational anomalies in downstream financial or OT systems | Vendor supply chain documentation artifacts: firmware version manifests from GPS receivers and satellite modems, any vendor security advisories or patch notifications received within the prior 12 months, and third-party security assessment responses — preserved to establish pre-incident supply chain posture if a compromise is later confirmed

Per-Action IR Details

Step 1: Inventory — catalog all operational dependencies on space-based services, including GPS timing for financial transaction sequencing, satellite communications for remote sites, and space-based positioning for logistics or operational technology environments (CIS 1.1: Establish and Maintain Detailed Enterprise Asset Inventory).

NIST Phase: Preparation

Reference: NIST 800-61r3 §2 — Preparation: Establishing IR capability requires knowing what assets and dependencies exist before an incident occurs

Controls: CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 3.2 (Establish and Maintain a Data Inventory), NIST IR-4 (Incident Handling)

Compensating: Use a spreadsheet-based dependency map combining outputs from 'traceroute', NTP pool query logs, and manual interviews with OT/facility teams. For GPS-disciplined clocks (e.g., Spectracom, Trimble, u-blox receivers), query SNMP or serial console for lock status and stratum level. Document each dependency: service type (GPS timing, VSAT uplink, LEO broadband), vendor, receiver hardware, and downstream systems that inherit the signal.

Evidence: This is a pre-incident preparation step with no live host state to alter; volatile capture is not applicable. Document current GPS lock status, NTP stratum hierarchy, and satellite uplink signal levels as a baseline — these values become the forensic reference point if timing drift or signal anomalies are later detected.

Step 2: Detection — identify which internal systems consume GPS timing signals, satellite uplinks, or space-based data feeds; log any anomalies in timing drift, signal loss, or unexpected command-and-control behavior at ground station interfaces (NIST AU-2: Event Logging; NIST SI-4: System Monitoring).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: Correlate timing anomalies and signal-layer events against established baselines to determine whether deviation indicates spoofing, jamming, or supply chain compromise

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy chrony or ntpd with logging enabled and alert on stratum changes greater than 1 level or time offsets exceeding 50ms using a cron-driven script querying 'chronyc tracking'. For ground station interfaces, capture SCADA/ICS command logs if accessible, or run Wireshark on the ground station LAN segment filtering for anomalous C2 protocol traffic (e.g., unexpected DVB-S2 encapsulated frames or RF modem management traffic on non-standard ports). Use osquery scheduled queries to identify NTP source changes on Linux hosts: 'SELECT * FROM time; SELECT * FROM etc_hosts;'

Evidence: Capture before any containment action: current NTP source and stratum from all GPS-disciplined devices ('chronyc sources -v' or 'w32tm /query /status'); ground station modem/receiver logs showing signal acquisition history, C/N0 (carrier-to-noise) values, and lock/unlock events; syslog or Windows Event Log entries (Event ID 37 — 'The time service has not been able to synchronize the system time') on any NTP-dependent server; and SCADA historian logs for any automated process that uses GPS-synchronized timestamps.

Step 3: Eradication — no patch action applies to this governance item; instead, review vendor security documentation for any space-based service providers in your supply chain and assess whether contractual security requirements address ground segment and link security (NIST SI-7: Software, Firmware, and Information Integrity).

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: In the absence of a patchable vulnerability, eradication focuses on removing systemic risk from the supply chain by validating that third-party space service providers meet documented security baselines for ground segment and uplink integrity

Controls: NIST SI-7 (Software, Firmware, And Information Integrity), NIST SI-5 (Security Alerts, Advisories, And Directives), CIS 2.2 (Ensure Authorized Software is Currently Supported)

Compensating: Create a vendor assessment checklist drawn from CISA's Space Systems Critical Infrastructure guidance and DHS S&T publications. For each satellite or ground station service provider, request evidence of: firmware signing and integrity verification for receiver hardware, encryption of command-and-control uplinks (minimum AES-128), and documented incident response contacts. Where vendors cannot provide documentation, flag the relationship for contractual renegotiation and document the risk acceptance decision in writing.

Evidence: Before concluding supply chain review, collect and preserve: current firmware version strings from all GPS receivers and satellite modems (queried via SNMP OID or vendor CLI); vendor-supplied software bill of materials (SBOM) if available; any prior vendor security advisories or change notifications received; and ground station network topology diagrams showing uplink encryption termination points. These constitute the pre-remediation baseline if a supply chain compromise is later confirmed.

Step 4: Recovery — establish resilience plans for degraded or denied space-based service scenarios; validate that backup timing, communications, and positioning sources exist for mission-critical operations dependent on GPS or satellite links (NIST IR-8: Incident Response Plan).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: Restore mission-critical operations by validating that backup timing, communications, and positioning sources are functional and that systems can fail over without data integrity loss

Controls: NIST IR-8 (Incident Response Plan), NIST IR-4 (Incident Handling), CIS 4.2 (Establish and Maintain a Secure Configuration Process for Network Infrastructure)

Compensating: Test GPS holdover on all stratum-1 NTP servers by physically disconnecting the GPS antenna and measuring drift rate over 24 hours using 'chronyc tracking' logged every 60 seconds via cron. For satellite communications backup, validate terrestrial failover (MPLS, cellular LTE/5G) by simulating VSAT outage and confirming that BGP or static route failover completes within defined RTO. Document results and gaps in a tabletop exercise report referencing the CISA Cross-Sector Space Systems Dependency guidance.

Evidence: Failover testing does not alter live production state if conducted on isolated test instances; however, if performed on production systems, capture before activating failover: current GPS lock status and PPS (pulse-per-second) output metrics, active BGP/OSPF routing table ('show ip route' or 'ip route show'), and NTP peer associations across all dependent servers. Post-failover, log the time delta between GPS-disciplined and backup timing sources to quantify timing accuracy degradation for downstream financial or OT systems.

Step 5: Post-Incident — monitor CISA space systems risk management guidance and DHS S&T publications for emerging baseline standards; incorporate space system dependencies into your next risk assessment cycle and flag any third-party providers lacking documented space segment security controls (NIST IR-4: Incident Handling; CIS 7.1: Establish and Maintain a Vulnerability Management Process).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: Conduct lessons-learned review, update risk assessments to reflect space system dependency exposure, and incorporate intelligence from CISA and DHS S&T into detection and governance posture

Controls: NIST IR-4 (Incident Handling), NIST IR-5 (Incident Monitoring), NIST IR-6 (Incident Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Subscribe to the CISA Critical Infrastructure Security advisories RSS feed and DHS S&T Cyber Security Division publication alerts — both are free. Use a shared wiki or ticketing system (e.g., Jira, Confluence, or a free GitHub project board) to track space system dependency risk items through the risk assessment cycle. Assign a named owner for each third-party space service provider relationship and set a calendar-triggered review every 90 days or upon receipt of any CISA space systems advisory.

Evidence: No volatile host state is altered in this phase; evidence capture focuses on documentation preservation: retain all vendor security assessment responses, risk acceptance decisions, and tabletop exercise reports with version control and timestamps. Archive CISA advisory notifications and DHS S&T publication downloads with receipt dates to demonstrate ongoing monitoring posture for audit purposes.

Detection Guidance

No active IOCs or exploitation indicators apply to this governance item. Detection priorities center on dependency visibility and anomaly monitoring. Log GPS timing deviation events on systems using PPS or NTP derived from GPS sources; unexpected drift can indicate spoofing or jamming. Monitor satellite communications links for unexpected outages, signal degradation patterns, or unauthorized connection attempts at ground station interfaces (NIST AU-6: Audit Record Review, Analysis, and Reporting). For organizations with direct ground segment operations, review access logs for command-and-control interfaces and validate integrity of uplink command sequences (NIST SI-4: System Monitoring). Organizations using space-derived timing for financial or industrial control systems should alert on NTP stratum changes or timestamp anomalies that could indicate upstream signal manipulation.

Framework Mappings

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.21** — Managing information security in the ICT supply chain

NIST-800-53R5

- **SR-2** — Supply Chain Risk Management Plan

NIST-CSF-2

- **GV.SC-01** — Cybersecurity supply chain risk management program

CIS-V8

- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC9.2** — Manages risks associated with vendors and business partners

Sources

Source	URL	Tier
Space Systems and Services | CISA	https://www.cisa.gov/topics/risk-management/space-systems	T1
[PDF] Time to Designate Space Systems as Critical Infrastructure - CSC 2.0	https://cybersolarium.org/wp-content/uploads/2023/04/CSC2.0_Report_...	T3
Developing security metrics for space systems: A study considering ...	https://www.sciencedirect.com/science/article/pii/S1874548225000666	T3
Space Based Platforms and Critical Infrastructure Vulnerability ...	https://kstatelibraries.pressbooks.pub/spacesystems/chapter/explora...	T3
US House debuts Space Infrastructure Act to designate space ...	https://industrialcyber.co/regulation-standards-and-compliance/us-h...	T3

Generated 2026-06-11 19:26 UTC by TJS Security Command Center