Policy Guidance: Cybersecurity Measures

CRSRA
Commercial Remote Sensing Regulatory Affairs

Guidance Circular

GC No: 960.9(a)-1
Subject: Guidance for Licensees - Cybersecurity measures
Date: August 16, 2022

Guidance Circulars (GC) are intended to provide guidance to entities subject to or potentially subject to the Land Remote Sensing Policy Act of 1992 (51 U.S.C. § 60101 *et seq.*) and the National Oceanic and Atmospheric Administration's (NOAA's) implementing regulations at 15 CFR Part 960. The contents of this document do not have the force and effect of law and are not meant to bind the public in any way. The document is only intended to provide clarity to the public regarding existing requirements under the law or agency policies.

Applicable Statute: 51 U.S.C. § 60121, 60122

Applicable Regulations: 15 C.F.R. 960.9(a)(1) and 960.10(a)(1)(i)

If you have suggestions for improving this GC, we invite you to provide feedback to NOAA's Commercial Remote Sensing Regulatory Affairs office (CRSRA) at crsra@noaa.gov, noting the number of the GC you are discussing in your email. Please note that responses by email are not anonymous and the entirety of the response, including the email address, attachments, and other supporting materials, may be disclosed pursuant to federal freedom of information law. Sensitive personal information, trade secrets, or financial information should not be included with the response.

Overview of Issue:
The Land Remote Sensing Policy Act of 1992 authorizes the Department of Commerce (delegated to NOAA) to license private entities to operate private remote sensing space systems, and prohibits the operation of private remote sensing space systems without such a license.

The implementing regulations, in some circumstances, require the implementation of certain cybersecurity measures. Compliance is subject to review by CRSRA.

First, all applicants whose system will have propulsion must affirm that the system has positive control (i.e., has implemented a way of ensuring that the propulsive system is always under the control of the licensee) which can entail cybersecurity measures. As stated in **Appendix A to Part 960** of the regulations, which provides the Application Information Required, all applicants whose system will have propulsion must:

> *Confirm by indicating below that there will be, at all times, measures in place to ensure positive control of any spacecraft in the system that have propulsion, if applicable to your system. Such measures include encryption of telemetry, command, and control communications or alternative measures consistent with industry best practice.*

Second, cybersecurity measures may be required depending on how CRSRA categorizes the license. The implementing regulations require categorization of licenses into one of these Tiers: Tier 1, Tier 2, or Tier 3. The Tier categorization results from CRSRA's determination about whether the system proposed will have the capability to collect unenhanced data substantially the same as unenhanced data already available from domestic or foreign entities or individuals (either licensed or not licensed by CRSRA). 15 C.F.R. § 960.6.

If a system is categorized as Tier 2 or Tier 3, the license will include conditions that require the licensee to have the ability to implement certain cybersecurity measures in connection with limited-operations directives. Specifically, section 960.9(a)(1) for Tier 2 systems and section 960.10(a)(1)(i) for Tier 3 systems, respectively, require the licensee to at all times have:

> *The ability to implement National Institute of Standards and Technology approved encryption, in accordance with the manufacturer's security policy, wherein the key length is at least 256 bits, for communications to and from the on-orbit components of the system related to tracking, telemetry, and control and for transmissions throughout the system of the data specified in the limited-operations directive; and*
>
> *Implementing measures, consistent with industry best practice for entities of similar size and business operations, that prevent unauthorized access to the system and identify any unauthorized access in the event of a limited-operations directive.*

If a system is categorized as Tier 3, there is the possibility that its license will also include custom Tier-3 temporary conditions to meet national security concerns or international obligations and policies—and these may include certain cybersecurity provisions. Section 960.10(b) provides:

> *The Secretaries of Defense and State shall determine whether any temporary license conditions are necessary (in addition to the standard license conditions in § 960.8) to*

meet national security concerns or international obligations and policies of the United States regarding that system.

Therefore, depending upon the licensee's specific mission and the tier categorization of the system, NOAA regulations may require the implementation of cybersecurity measures to ensure:

- Positive spacecraft control;
- Successful implementation of limited-operations directives; and
- Addressing other national security concerns or international obligations and policies based on the unique capabilities of the system.

CRSRA Approach to Cybersecurity

This Guidance Circular provides CRSRA's view of successful cybersecurity measures that are relevant (and potentially applicable) to holders of private remote sensing space system licenses. In that context, it provides cybersecurity policy guidance from the President and implementation guidance from designated agencies and industry experts that together constitute best industry desired outcomes and standards. CRSRA understands that the best industry practices call for licensees to apply cybersecurity measures tailored to their specific mission requirements, applicable regulations and license requirements, and space system design and operation. This Guidance Circular also identifies a comprehensive process that space operators can follow to develop and implement appropriate cybersecurity plans, designs, and practices compliant with NOAA requirements to develop and operate a system that is resilient to cyber attacks.

Accordingly, this Guidance Circular is organized as follows:

I. Satellite Systems Background
II. Space Policy Directive 5: Cybersecurity Principles for Space Systems
III. Applying SPD-5: Cybersecurity Implementation
IV. Introduction to the National Institute of Science and Technology Cybersecurity Framework
V. Process to Develop Cybersecurity Defense Tailored to Your Needs
    A. Overall Checklist
    B. Surveying Threats
    C. Identifying Risk
    D. Protecting the Space Segment
    E. Selecting Controls
        1. General list of controls
        2. Supply chain protection and controls
        3. Satellite link protection and controls
        4. Space segment protection and controls
        5. Cloud controls
    F. Key Points - Summary
    G. Documentation References
VI. Additional References
    A. Appendix A: Mapping SPD-5 cybersecurity principles to NIST controls

B. Appendix B: 40 Questions to consider when understanding cyber risks/gaps for a space system.
C. Appendix C: Overview of DOD and NASA cybersecurity policy documents

I. Satellite System Background

Figure 1 below identifies a typical configuration for a private remote sensing space system. A space system comprises three segments; a space segment, a ground segment, and a link segment interconnecting the ground and space segments with wired and wireless communication elements. The space complement is further decomposed into a spacecraft bus and mission payload, and the ground network into an operations center and a data center. The system is controlled from an element of the ground segment known as a Satellite Operations Center (SOC), also called a Mission Control Center or MCC. The SOC sends commands to the space segment to task imaging collection (the remote sensing instrument) and control other satellite systems. These commands are routed using terrestrial telecommunications connectivity to selected Remote Ground Terminals (RGTs). The space segment sends telemetry data back through the RGT and on to the SOC. After payload (remote sensed - RS) data is collected by the imaging instrument on the spacecraft it is stored onboard until it can be sent to the ground. RGTs used for downlinking data may or may not coincide with Telemetry, Tracking, and Command (TT&C) RGTs as the former require a high speed connection to handle the large volumes of data. The remote sensed (RS) data is stored either on private servers owned by the applicant or, more commonly, on equipment owned and maintained by one of the “cloud” providers such as AWS, Azure, Google Cloud, IBM Cloud, Oracle Cloud, etc. The data is usually processed to various levels of refinement corresponding to levels 0-2 of environmental data, wherein it is corrected for limitations of the instrument and atmospheric alterations, geo-referenced, turned into images, and/or assessed by Artificial Intelligence (AI) software. The data may be made available to customers or stored and used internally by the operator for analytics purposes.

As used here, RGTs are satellite uplink and/or downlink terminals located around the world functioning as bent pipes to forward data in each direction and may or may not have any human operators but require electrical power, telecommunications connections, and in-country regulatory approval. Data is not stored permanently, but may be stored temporarily to accomplish the function of reliable (positively acknowledged) transmission.

Outside companies contracted to provide services such as mission operations or data hosting or processing, telecommunications, and ground terminal services are all considered part of the satellite operator's network.

Telemetry refers to data packets containing health and status information of the satellite and the imaging instrument, and command acknowledgements.

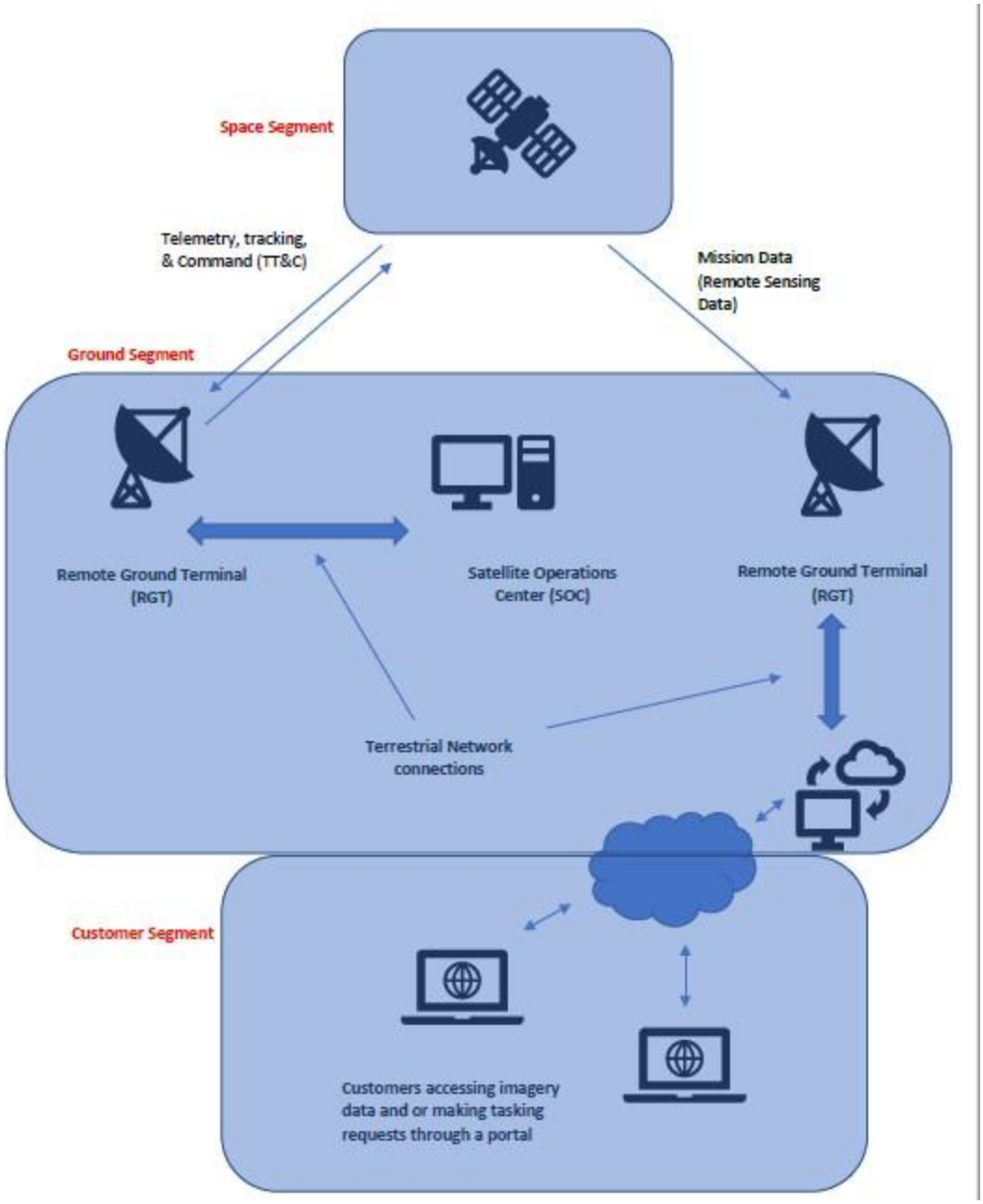


Figure 1. Remote System Satellite System *Source: NOAA.*

II. Space Policy Directive 5: Cybersecurity Principles for Space Systems

Space Policy Directive 5 (SPD-5)[1], titled "Cybersecurity Principles for Space Systems," is a Presidential memorandum published in 2020 that establishes key cybersecurity principles to guide and serve as the foundation for America's approach to the cyber protection of space systems. It directs U.S. Government agencies to work with commercial companies consistent with the principles in the SPD to enhance cyber resilience[2] by further defining best practices, establishing cybersecurity informed norms, and promoting improved cybersecurity behaviors throughout the Nation's industrial base for space systems. This section of the Guidance Circular serves as an outline of the relevant definitions and provisions in SPD-5.

Note: While SPD-5 promulgates space cybersecurity principles and desired behaviors, implementation of SPD-5 relies on subsidiary regulations and mapping its objectives to relevant standards, controls, and guidance, as discussed in the following sections and Appendix A.

Section 2 of SPD-5 provides several definitions. Relevant here, SPD-5 defines "Positive Control" as:

> *[T]he assurance that a space vehicle will only execute commands transmitted by an authorized source and that those commands are executed in the proper order and at the intended time.*

Section 3 of SPD-5 states that cybersecurity should be integrated into all phases of space system development and across the full system lifecycle.

Section 4 of SPD-5 identifies cybersecurity principles for space systems to guide and serve as the foundation for an approach to the cyber protection of space systems.

Section 4(a) of SPD-5 states that space systems and their supporting infrastructure, including software, should be developed and operated using risk-based, cybersecurity-informed engineering and identifies specific goals and behaviors.

Cybersecurity risk[3] is determined by the interaction of factors including: the nature of the cyber threat (the attacker's capabilities and motivation), the vulnerabilities of the space system, and the impact of a cyber attack (what is the criticality of the information or assets at risk). Organizational risk occurs to organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.

---

[1] Link to SPD-5: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

[2] Cyber resiliency (also referred to as cyber resilience) is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. *See* MITRE Corp., *Cyber Resiliency FAQ* (2017). Link: https://www.mitre.org/sites/default/files/PR_17-1434.pdf

[3] Adapted from the generic risk model in Figure 3, NIST Special Publication 800 Revision 1, Guide for Conducting Risk Assessments. Link: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

Section 4(b) of SPD-5 provides more detailed principles for what should be included in a cybersecurity plan. Specifically, Section 4(b) states:

> *Space system owners and operators should develop and implement cybersecurity plans to ensure retention or recovery of **positive control of space vehicles** and ensure the integrity, confidentiality, and availability of critical functions and the missions, services, and data they enable and provide.*

(emphasis added). It further instructs that at a minimum, space system owners and operators should consider, based on risk assessment and tolerance, incorporating various elements in their plans. SPD-5 identifies these elements as:

(i) **Protection against unauthorized access to critical space vehicle functions** including the use of **authentication [and] or encryption measures** designed to remain secure against existing and anticipated threats during the entire mission lifetime;
(ii) **Physical protection measures** designed to reduce the vulnerabilities of a space vehicle's **command, control, and telemetry** receiver **systems**;
(iii) **Protection against communications jamming and spoofing**;
(iv) **Protection of ground systems,** operational technology, and information processing systems through the adoption of **deliberate cybersecurity best practices**. **This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework** to reduce the risk of malware infection and malicious access to systems, including from insider threats. Such practices include **logical or physical segregation; regular patching; physical security; restrictions on the utilization of portable media; the use of antivirus software; and promoting staff awareness and training** inclusive of insider threat mitigation precautions;
(v) **Adoption of appropriate cybersecurity hygiene practices**, **physical security** for automated information systems, and **intrusion detection** methodologies for system elements[4] such as information systems, antennas, terminals, receivers, routers, associated local and wide area networks, and power supplies; and
(vi) **Management of supply chain risks**.

Section 4(d) of SPD-5 provides the principles for **information sharing.** The section states:

> ***Space system owners and operators should collaborate** to promote the development of best practices, to the extent permitted by applicable law. **They should also share threat**, **warning**, and incident **information** within the space industry, using venues such as **Information Sharing and Analysis Centers** to the greatest extent possible, consistent with applicable law.*

[4] Include 3rd party infrastructure such as service or data hosting services, telecommunications, providers and ground terminal services.

(emphasis added).

Finally, Section 4(e) of SPD-5 addresses **tailoring measures to reduce undue burden** to the operator. Specifically, it states:

> *Security measures should be designed to be effective while permitting space system owners and operators to manage appropriate risk tolerances and minimize undue burden, consistent with specific mission requirements, United States national security and national critical functions, space vehicle size, mission duration, maneuverability, and any applicable orbital regimes.*

III. Applying SPD-5: Cybersecurity Implementation

While informative, SPD-5 is not intended to be used as a set of actionable controls (technical or operational practices) that an operator or designer can read and directly implement. Implementation of SPD-5 instead relies on related regulations and the conscious mapping of objectives to relevant standards, controls, and guidance.

Actionable guidance is currently lacking for space system developers, mission owners, and operators concerning cybersecurity threats and defensive countermeasures. Existing policy guidance is too abstract to address cybersecurity threats in a tangible manner. Conversely, extremely specific and technical lists of security controls for space systems are not directly traceable to mission needs and do not offer alternative defensive solutions. These lists risk stifling efforts to ensure controls are being implemented effectively and commensurate with the threats space systems face and thus not overburdening enterprises.

This Guidance Circular helps licensees by identifying several resources that bridge the policy underlying SPD-5 to technical controls for space systems. First, licensees should familiarize themselves with the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) which provides a method to identify relevant controls to protect your business and is discussed in Section IV below.

Second, licensees can review the paper titled "Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles."[5] The paper concludes that as threats against space systems continue to evolve, new technology is introduced to the domain, and space systems become further integrated into critical infrastructure that society relies on, assessing and addressing risks must be continuous. The concepts introduced in the paper are intended to enable actionable risk management through the identification of applicable and relevant

[5] Nicholas Tsamis, Brandon Bailey and Gregory Falco, AIAA 2021-4051, *Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles* (April 29, 2021).

cybersecurity controls. The example use case in the paper demonstrates how identifying needs related to one function from the NIST CSF can help inform relevant and necessary cybersecurity capabilities in others. The analysis and documentation process discussed in this paper should be customized for a designer/operator's specific mission system and then extended to all other space vehicle subsystems in order to capture additional cybersecurity needs. This process helps to identify focus areas for addressing outstanding cybersecurity issues where improper or inapplicable controls may be in use. High level directives such as SPD-5 provide well-intentioned cybersecurity goals for space system owners. Reviewing the artifacts presented in the paper helps to easily identify where such guidance may be incomplete. The proposed process can help ensure that cybersecurity attention is focused where it matters most - to protect the mission objective. This should help to shift mission owner mentality away from entirely relying on baseline control sets, to a more thoughtful analysis where security control identification is tailored to the mission needs.

Third, licensees should work through Section V below to identify the truly critical elements of their system and business and the extent of resources to protect them.

Fourth, Appendix A of this Guidance Circular, in subsections 4-8, maps out the SPD-5 principles and desired end-states to NIST controls. This will be very helpful during completion of the CSF, after critical remote sensing and business functions and data have been identified and appropriate protection methods are sought.

IV. Introduction to the National Institute of Science and Technology Cybersecurity Framework

The National Institute of Science and Technology Cybersecurity Framework (NIST CSF)[6] provides a methodology for entities to manage cybersecurity risk by **identifying** cyber threats to your company/remote sensing system, your vulnerabilities to cyber threats, and the impact to you (and possibly others) if they are compromised. The CSF then guides users through selecting corresponding **protection**, **detection**, **response** and **recovery** strategies and actions.

The process of applying the CSF entails surveying the threat environment and vectors, inventorying systems and assets, and determining system vulnerabilities. Note that it is assumed that an entity has already determined their risk profile (see section V.C below). The CSF is not specific to space systems, but can be applied to space systems and NIST is developing profiles which apply the CSF to commercial space systems.

[6] *See* NIST, *Framework for Improving Critical Infrastructure Cybersecurity* (Aug. 16, 2018). Link: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pd. More generally the NIST CSF is at: https://www.nist.gov/cyberframework.

The CSF application profiles which denote a process for commercial space systems include:

Document Number	Title	Description
NIST IR 8270	Introduction to Cybersecurity for Commercial Satellite Operations[7]	Provides a sample CSF profile for the space segment of commercial space systems.
NIST IR 8401	Satellite Ground Segment: Applying the Cybersecurity Framework to Assure Satellite Command and Control[8]	Provides a sample CSF profile for the ground segment of commercial space systems.

V. Process to Develop Cybersecurity System Tailored to Your Needs

A. Space Operator Cybersecurity Protection Checklist

CRSRA recommends licensees review the following roadmap when developing their cybersecurity system for spacecraft systems and operations.

Note: this generally follows the *National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity Version 1.1* (the Cybersecurity Framework or CSF process - discussed above in Section IV).

Task	Description	Notes
Review and Model Threat Intelligence for Relevant Cyber Threats	See Section V.B below for resources	

[7] NISTIR 8270: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8270-draft2.pdf
[8] NISTIR 8401: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8401.ipd.pdf

Determine Your Space System Risk Profile	Follow the process identified in sub-Section C below. This includes assaying the following, for each system component; criticality, vulnerability, and impact of compromise, and then developing a set of scenarios showing risk and resultant effects.	If your system was assigned Tier 1, and if your spacecraft does not have propulsion, there are no applicable NOAA cybersecurity requirements. Using this circular to develop and operate a cyber resilient space system is still recommended.
Select Appropriate Controls	Work through the NIST CSF using NIST IR 8270 and 8401 and select appropriate controls for your system from NIST SP 800-53 Rev 5. Assume your network can be compromised even with strong protections. Plan a layered defense that will protect your most critical data and functions even when an attacker is operating inside your network.	Security controls exist to reduce or mitigate risk. They include any type of policy, procedure, technique, method, solution, plan, action, or device designed to help do so. Examples include firewalls, surveillance systems, and antivirus software. NIST IR 8270 and 8401 apply CSF to space systems, please refer to Section IV. For NIST SP 800-53 Rev 5 refer to Section V.D.
Protect the Space Segment	Include specific protections for the space segment, refer to Section V.D.4.	
Implement Cloud Controls (if needed)	If using a cloud provider for data storage or other functions, review and activate appropriate cyber protection options from the provider.	
Implement Propulsion Cybersecurity Controls (if needed)	If your spacecraft has propulsion, your overall cybersecurity design and practices should ensure positive control over the spacecraft.	Positive control is defined in SPD-5 (Section 2 above) and entails a comprehensive approach to cybersecurity

Space Link Protection	See Section V.D.3 below.	If you are NOAA Tier 2 or 3, ensure your system meets specific compliance requirements for space link protection.
Keep Up with Evolving Threats	Update threat information and system risk profile over time.	

Note: the list of questions in Appendix B may be helpful as you get started.

B. Surveying Cyber Threats

Updated information regarding cyber threats to space systems can be obtained from a number of sources, including:

- The Space Information Sharing and Analysis Center (ISAC)[9] member-driven resource for private space stakeholders
- The Department of Homeland Security's (DHS) CyberSecurity and Infrastructure Security Agency (CISA) Shields-Up program[10]
- The National Security Agency (NSA)[11]

Once space cyber threats are known, they can be modeled for your system. For information on the the basics of data-centric system threat modeling that be used as part of the risk management process, you can refer to:

- **NIST SP 800-154,** *Guide to Data-Centric System Threat Modeling*[12]
- ***Cybersecurity Protection for Spacecraft: A Threat Based Approach***, TOR-2021-01333 Rev A[13] Section 3: Threat Informed Requirements for Spacecraft

Both documents examine data-centric system threat modeling, which is threat modeling focused on protecting particular types of data within systems.

[9] Space ISAC website: https://s-isac.org/
[10] DHS CISA *Shields-Up* program: https://www.cisa.gov/shields-up and https://www.cisa.gov/information-sharing-and-awareness
[11] NSA Cyber Advisories: https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/
[12] NIST SP 800-154, *Guide to Data-Centric System Threat Modeling* (March 2016). Link: https://csrc.nist.gov/publications/detail/sp/800-154/draft
[13] Brandon Bailey, The Aerospace Corp. Cyber Assessment and Research Department (CARD) (April 29, 2021). Link: https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft--A%20Threat%20Based%20Approach.pdf

C. Determining Risk Profile

Refer to NIST **Special Publication (SP) 800-30 Revision 1** *Guide for Conducting Risk Assessments*[14] and also consider such factors noted in the table below to determine your overall risk profile. The NIST Guide describes risk as a combination of threat and system factors. The generic risk model in the NIST Guide will guide operators through the risk factors. In applying the NIST Guide, users will:

- Assess criticality of each system component. Include leased service(s) such as telecommunications, hosting services, and ground stations.
- Assess likelihood of (vulnerability to) compromise of each component.
- Assess impact of compromise of each component.

Operators can then develop a set of scenarios showing risk and resultant effects for use in deciding where to concentrate protection.

Table 1. Selected Space Operator Cybersecurity Risk Elements (Non-inclusive list)

Risk Factor	Classes	Risk Rating
NOAA Tier (data sensitivity)	Tier 1 Tier 2 Tier 3	Low-Medium Medium-High High
Satellite propulsion	Yes No	Medium-High Low
Level of proprietary information /Intellectual Property (IP) stored in the enterprise network	Yes No	High Low
Own/operate a Satellite Control Center (SCC)	Yes No	High Low
Own/operate a Space Data repository/archive	Yes No	Medium-High Low
Use of 3rd party services for service or operations hosting, telecommunications, ground station functions. Risk depends upon network design and the security posture of the third party.	Public Shared Private	High Medium Low

[14]NIST SP 800-30 Rev. 1, *Guide for Conducting Risk Assessment* (Sep. 2012). Link: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-30r1.pdf

D. Selecting Controls

1. General list of controls

Private remote sensing space system operators should consider implementation of, and NOAA Tier 3 licensees may be required to implement, portions of (specific controls identified in) these NIST standards:

Document Number	Title	Description
NIST SP 800-171 Rev. 3	Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations[15]	Provides recommended requirements for protecting the confidentiality of controlled unclassified information to ensure government information located on contractors' networks is secure.
NIST SP 800-172	Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171[16]	Provides best practice processes and security controls to safeguard sensitive information on non-federal systems.
NIST SP 800-53 Rev. 5	Security and Privacy Controls for Information Systems and Organizations[17]	Provides a catalog of security and privacy controls for federal information systems except those related to national security.

2. Supply chain protection and controls

Satellite system developers rely on a wide variety of hardware and software components sourced from around the world, any of which could be an entry point for malware or other cyber risk to enter the system. Therefore, supply chain security is paramount.

Contracting with outside companies to provide services such as service or data hosting or processing, telecommunications, and ground terminal services should be considered part of the satellite operator's network and the operator is responsible for vetting them and ensuring that they comply with any applicable cyber security requirements.

To help secure the supply chain, these NIST documents can provide assistance:

[15] NIST SP 800-171: https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
[16] NIST SP 800-172: https://csrc.nist.gov/publications/detail/sp/800-172/final
[17] NIST SP 800-53 Rev. 5: https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final

Document Number	Title	Description
NIST Interagency/Internal Report (NISTIR) - 8276	Key Practices in Cyber Supply Chain Risk Management: Observations from Industry[18]	Provides a high-level summary of practices deemed by subject matter experts to be foundational to an effective cyber supply chain risk management program.
NIST CSWP 02042020-2	Case Studies in Cyber Supply Chain Risk Management: Anonymous Consumer Electronics Company[19]	Provides a review of the cyber supply chain risk management measures of an American manufacturer of high-end audio equipment.
NIST CSWP 02042020-1	Case Studies in Cyber Supply Chain Risk Management: Summary of Findings and Recommendations[20]	Provides a summary of key findings from a deep dive into the experience of six organizations regarding cyber supply chain risk management programs.
NIST Special Publication (NIST SP) - 800-161	Supply Chain Risk Management Practices for Federal Information Systems and Organizations[21]	Provides guidance to federal agencies on identifying, assessing, and mitigating information and communications technology supply chain risks at all levels of their organizations.

[18] NIST Interagency/Internal Report (NISTIR) - 8276: https://www.nist.gov/publications/key-practices-cyber-supply-chain-risk-management-observations-industry
[19] NIST CSWP 02042020-2: https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-consumer-electronics-company
[20] NIST CSWP 02042020-1: https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-summary-findings-and-recommendations
[21] NIST Special Publication (NIST SP) - 800-161: https://www.nist.gov/publications/supply-chain-risk-management-practices-federal-information-systems-and-organizations

3. Satellite link protection and controls

For Tier 2 and 3 systems, the ability to enable Advanced Encryption Standard (AES) with a 256 bit key for TT&C links is required. For space systems of any Tier equipped with propulsion, user authentication using encryption is the easiest method to ensure positive control. Other means can further aid in ensuring positive control, though constitute only a portion of an overall solution. For guidance from NIST regarding authentication and encryption:

Document Number	Title	Description
NIST AC-18(1)	Authentication and Encryption[22]	Guidance on authentication and encryption and links to related controls. **Note**: The following are suggested controls for protecting the Command and Telemetry (TT&C) links of space systems: IA-5(7), SI-10(3), AC-2(11), AC-3(10), AU-3(1), IA-5, IA-7, SC-10, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-28(1), SC-7, SC-7(11), SC-7(18), SI-3(9), SI-10, SI-10(5), AC-17(1), AC-17(2), AC-18(1)
NIST FIPS - 197	Advanced Encryption Standard (AES)[23]	Guidance on the AES standard.
N/A	The Advanced Encryption Standard Algorithm Validation Suite[24]	Guidance and tests on encryption algorithm validation for implementing FIPS -197.

4. Space segment protection and controls

The level of cyber risk present at the space segment / spacecraft is somewhat lower than the space link or the ground segment due to the difficulty of accessing it, and the historical practice of customized hardware and software design which challenges an adversary to investigate. As space designs become more modular, however, this source of protection is reduced. In any case, supply chain threats provide a means to embed malware inside the spacecraft without needing to break encryption or deploy jamming infrastructure. In addition to securing the supply chain, there are a number of measures which can provide protection and

[22] Authentication and Encryption: https://csf.tools/reference/nist-sp-800-53/r5/ac/ac-18/ac-18-1/
[23] NIST CSWP 02042020-2: https://www.nist.gov/publications/case-studies-cyber-supply-chain-risk-management-anonymous-consumer-electronics-company
[24] The Advanced Encryption Standard Algorithm Validation Suite: https://csrc.nist.rip/groups/STM/cavp/documents/aes/AESAVS.pdf

detect intrusions to the space segment. Cybersecurity controls, design features, and other measures to aid protection of the spacecraft are noted in TOR-2021-01333 and the other documents referenced below. At a minimum, spacecraft operators should strongly consider logging all commands received and executed by the spacecraft so that any intrusions are documented for later troubleshooting. For more sophisticated protection, operators may install on-board AI software which looks for commands outside of normal usage and stops them from execution and consider the additional measures identified below the table.

Document Number	Title	Description
TOR-2021-01333 Rev A	Cybersecurity Protection for Spacecraft: A Threat Based Approach[25]	Report outlining concepts of defense-in-depth protection necessary to protect spacecraft, and then a threat-oriented approach to space cyber risk assessment.
AD1087142	Guidelines for Secure Small Satellite Design and Implementation: FY18 Cyber Security Line-Supported Program[26]	This document lays out the problem space for cybersecurity in this domain, derives design guidelines for future secure space systems, proposes an exemplar architecture that implements the guidelines, and provides a solid starting point for near-term and future satellite processing
SSC16-IV-6	Towards Effective Cybersecurity for Modular, Open Architecture Satellite Systems[27]	The paper describes an approach to overlaying cyber security design and testing into the small satellite acquisition lifecycle. Lessons learned from SCADA/ICS cybersecurity research are described, along with descriptions of cybersecurity tools and methods applicable to small satellites. Finally, ongoing cybersecurity testing of a BeagleBone Black processor is described, along with initial findings and comments about how to harden the processor against cyberattack.

[25] Brandon Bailey, TOR-2021-01333 Rev A, The Aerospace Corporation, 2021, 29 April 2021. Link: /https://aerospace.org/sites/default/files/2022-07/DistroA-TOR-2021-01333-Cybersecurity%20Protections%20for%20Spacecraft--A%20Threat%20Based%20Approach.pdf

[26] Ingols, K. W. Skowyra, R. W. Lincoln Labs, *Guidelines for Secure Small Satellite Design and Implementation: FY18 Cyber Security Line-Supported Program* (Feb. 6, 2019). Link: https://apps.dtic.mil/sti/citations/AD1087142

[27] Daniel E. Cunningham, Geancarlo Palavinicni Jr., and Jose Romero-Mariona of SPAWAR Systems Center Pacific, *Towards Effective Cybersecurity for Modular Open Architecture Satellite Systems* (2016). Link: https://digitalcommons.usu.edu/smallsat/2016/TS4AdvTech1/6/

DEF CON 28 presentation.	Aerospace Village: Exploiting Spacecraft[28]	The presentation provides a useful overview of the cybersecurity risks to spacecraft and the general approach to manage it.

TOR-2021-01333 reviews the following measures:

- Leverage defense-in-depth architecture across both the spacecraft and ground system to counter the applicable threats
- Protecting the TT&C link from intrusion via encryption/authentication with robust key management as well as jamming/spoofing attacks. Additionally, ensuring protection on-board the spacecraft to limit ability and impact of authentic ground system to be used to attack spacecraft
- Intrusion detection and prevention leveraging signatures and machine learning to detect and block cyber intrusions onboard spacecraft
- Logging onboard the spacecraft to verify legitimate operations and aid in forensic investigations after anomalies
- A supply chain risk management program to protect against malware inserted in parts and modules
- Software assurance methods within the software supply chain to reduce the likelihood of cyber weaknesses in flight software and firmware
- Use of Root-of-Trust (RoT) [a set of functions and commands accessed by the computing module that it trusts - ie are stored in permanent memory] to protect software and firmware integrity
- A tamper-proof means to restore the spacecraft to a known good cyber-safe mode
- Lightweight cryptographic solutions for use in smallsats

5. Cloud controls

If using a cloud provider for data storage or other functions, review and activate appropriate cyber protection options from the provider.

E. Space Cyber Defense Key Points

- Threat informed risk-based cyber security engineering is needed
    - Security is an engineering problem
- A whole organizational commitment with living processes, systems, and training is required
- All three segments (space, ground, link) are different and require different security
    - Protect the ground system from cyber attack
    - Protect the ground-to-space command link and any cross-links

[28] Brandon Bailey at DEF CON 28, Aerospace VIllage Presentation: Exploiting Spacecraft (Aug. 7, 2020). Link: https://www.youtube.com/watch?v=b8QWNiqTx1c

    - Establish a robust strategy for cryptography key management. If key management is poor or keys are stolen, encryption provides little value on protection
- A layered defense is needed - for each system segment
    - Assume attackers will get past the perimeter of any segment
    - Understand threats and vulnerabilities at each network layer
    - Use repeated levels of segmentation, least privilege, encryption, authentication, and other controls at interfaces to constrain mobility of the attacker within the network element and protect the critical data or functionality
    - Ground security with TRANSEC or COMSEC is not sufficient
- Protect the **supply chain** and the development environment from compromise.
- Given the complex nature of space vehicle supply chains and the expanding commercialization of space, protecting the supply chain is becoming of utmost importance
- Ensure **secure software development** procedures are in place to prevent design flaws, insecure logic, and coding defects that could affect the flight software
- Design for **cyber resiliency on-board the satellite** to ensure proper detection, recovery, and response leveraging automation, machine learning and other forms of artificial intelligence

F. Cybersecurity Document Hierarchy

This Guidance Circular references numerous documents external to CRSRA. Some of these documents present broad Federal policy and others provide tailored information for specific operations. To help understand the significance of the different references, CRSRA has prepared the following document flow-down or hierarchy for space cybersecurity protection. In general, the hierarchy from broad references to specific is as follows:

Policy Directives --> Acquisition Requirements --> Cybersecurity Standards

Policy Directives

- The highest level U.S. policy document applicable to commercial space is Space Policy Directive 5 (SPD-5): Cybersecurity for Space Systems.[29]

SPD-5 establishes key cybersecurity principles to guide and serve as the foundation for America's approach to the cyber protection of space systems. Further, SPD-5 provides guidance on the protection of space assets and supporting infrastructure from evolving cyber threats and mitigates the potential for the creation of harmful space debris resulting from malicious cyber activities.

[29] SPD-5: https://trumpwhitehouse.archives.gov/presidential-actions/memorandum-space-policy-directive-5-cybersecurity-principles-space-systems/

Acquisition Requirements
Acquisition agencies such as NASA and DoD also levy cybersecurity requirements on vendors - these help ensure data integrity, provide mission assurance, and manage cyber risk to the procuring agency. Holders of NOAA licenses should consider requirements from each regulatory or acquisition agency independently and verify compliance with all applicable requirements. Appendix C provides information regarding DoD and NASA cybersecurity documentation.

Cybersecurity Standards
Standards bodies such as NIST and the Consultative Committee for Space Data System Standards (CCSDS) develop cybersecurity standards and guidance that can be used by businesses and acquisition agencies seeking to improve their cybersecurity posture. The Office of Management and Budget (OMB) mandates that all federal agencies implement NIST's cybersecurity standards and guidance for non-national security systems.

NIST Cybersecurity Standards
NIST has a family of relevant standards, frameworks, controls, and application guides. The foundational NIST cybersecurity framework documents are:

- *Framework for Improving Critical Infrastructure Cybersecurity* V1.1[30] (the CSF)
- *Risk Management Framework for Information Systems and Organizations (the RMF)*
    - *https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf*

Both of these present frameworks for entities to address and manage cybersecurity risk in a cost-effective way, based on business and organizational needs. The CSF focuses on using business drivers to guide cybersecurity activities and considers cybersecurity risks as part of the organization's overall risk management processes. Both the CSF and RMF pull from the same security best practices, and there are other similarities between them, however a key difference is that compliance with the RMF is mandated for federal agencies while the CSF originated as a voluntary commercial framework (e.g., with the CSF there is no Authorization step and it does not assume there is a Designated Approving Authority). Below is a visual of the use of the RMF vs the CSF.

[30] The NIST CSF was developed under Executive Order (EO) 13636

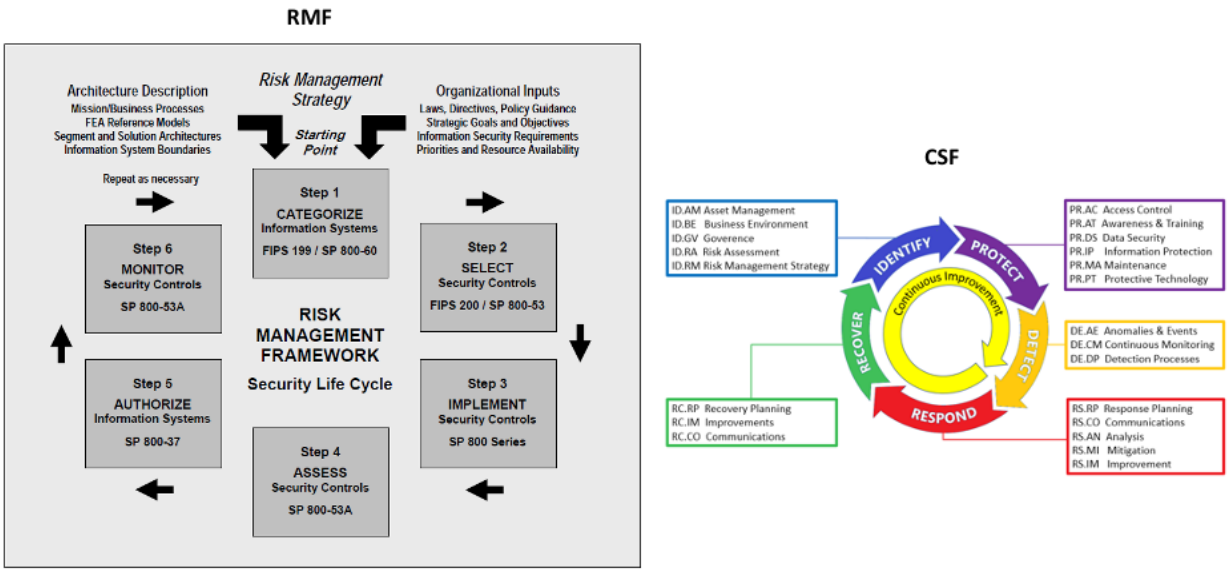


Image Source: *Nicholas Tsamis, Brandon Bailey and Gregory Falco, AIAA 2021-4051, Translating Space Cybersecurity Policy into Actionable Guidance for Space Vehicles.*

The NIST CSF, other NIST documents regarding cybersecurity controls and standards, and the application profile documents for commercial space are described in more detail, along with references, in **Sections IV and V** of this document.

CCSDS Standards

Another source of cybersecurity protection standards for space, especially for the space-ground link, is the Consultative Committee for Space Data System Standards (CCSDS). Standards for link and data protection can be viewed here:

- **CCSDS 350.5-G-1** Space Data Link Security Protocol - Summary of Concept and Rationale
  - Link: https://public.ccsds.org/Pubs/350x5g1.pdf
- **CCSDS 352.0-B-2** Cryptographic Algorithms
  - Link: https://public.ccsds.org/Pubs/352x0b2.pdf
- **CCSDS 355.0-B-1** Space Data Link Security (SDLS) Protocol
  - Link: https://public.ccsds.org/Pubs/355x0b1.pdf
- **CCSDS 356.0-B-1** Network Security Layer
  - Link: https://public.ccsds.org/Pubs/356xb1.pdf
- **CCSDS 357.0-B-1** Authentication Credentials
  - Link: https://public.ccsds.org/Pubs/357x0b1.pdf

Opportunity for Feedback:

We welcome any feedback you may have about this GC. Please contact CRSRA at crsra@noaa.gov.

Appendix A

Mapping of SPD-5 Cybersecurity Principles to NIST Controls

SPD-5 Principles Summary

The following table provides an outline of the SPD-5 Principles broken down by their identifier (ID) and provides both the high level concept and a detailed description of the principle.

SPD-5 Principles- Detailed

ID	High Level Concepts	More Detailed Description
i	**Protect against unauthorized access to Vehicle**	Protection against unauthorized access to critical space vehicle functions. This should include safeguarding command, control, and telemetry links using effective and validated authentication or encryption measures designed to remain secure against existing and anticipated threats during the entire mission lifetime;
ii	**Provide physical protection measures for TT&C**	Physical protection measures designed to reduce the vulnerabilities of a space vehicle's command, control, and telemetry receiver systems;
iii	**Defend communications**	Protection against communications jamming and spoofing, such as signal strength monitoring programs, secured transmitters and receivers, authentication, or effective, validated, and tested encryption measures designed to provide security against existing and anticipated threats during the entire mission lifetime;
iv	**Guard ground systems**	Protection of ground systems, operational technology, and information processing systems through the adoption of deliberate cybersecurity best practices. This adoption should include practices aligned with the National Institute of Standards and Technology's Cybersecurity Framework to reduce the risk of malware infection and malicious access to systems, including from insider threats. Such practices include logical or physical segregation; regular patching; physical security; restrictions on the utilization of portable media; the use of antivirus software; and promoting staff awareness and training inclusive of insider threat mitigation precautions;
v	**Practice cybersecurity hygiene**	Adoption of appropriate cybersecurity hygiene practices, physical security for automated information systems, and intrusion detection methodologies for system elements such as information systems, antennas, terminals, receivers, routers, associated local and wide area networks, and power supplies;
vi	**Manage supply chain risks**	Management of supply chain risks that affect the cybersecurity of space systems through tracking manufactured products; requiring sourcing from trusted suppliers; identifying counterfeit, fraudulent, and malicious equipment; and assessing other available risk mitigation measures.

Existing Content Mapped to SPD-5 Principles

Threat-based perspective

TOR-2021-01333 REV A, referenced in Section V.D.4 above, outlined how to perform risk analysis by leveraging an example methodology backed by a generic space specific threat model. Other methodologies can be used, but a key aspect is analyzing system design against the predefined list of threats/vulnerabilities. The benefit of the information in this appendix is in providing a resource for guidance using available unclassified threat information from TOR 2021-01333 and cross referencing it with SPD-5 security principles.

The threats/vulnerabilities have a custom identifier in the form of SV-XX-# which can be used to search/sort through various tables/resources in TOR-2021-01333. SV stands for Space Vehicle and the XX vary between the following abbreviations:

- AC = Access Control
- IT = Integrity
- AV= Availability
- MA = Mission Assurance
- CF = Confidentiality
- SP = Supply Chain
- DCO = Defensive Cyber Operations

The subsequent tables/figures depict the information being cross referenced to generic space threat models from the same TOR. The resources in this appendix are listed in tabular format. The following columns are listed in the table.

- ID = Threat/Vulnerability ID from TOR-2021-01333
- Threat/Vulnerability High Level Description = Natural language description maintaining wording from source material
- SPD-5 (i)-(vi)) = ID for SPD-5 principles as defined on previous page
- High Level Best Practices = Basic best practices to consider to mitigate threat vectors for SVs or a Cybersecurity Program
- Control Tag Mappings = Identifier/tag from NIST SP 800-53/CNSSI 1253[31]

[31] CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems. Link: https://www.dcsa.mil/portals/91/documents/ctp/nao/CNSSI_No1253.pdf

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-AC-1	Attempting access to an access-controlled system resulting in unauthorized access	x	x					The SV should protect the commanding capability from intrusion.	IA-5(7), SI-10(3), AC-2(11), AC-3(10), AU-3(1), IA-5, IA-7, SC-10, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-28(1), SC-7, SC-7(11), SC-7(18), SI-3(9), SI-10, SI-10(5), AC-17(1), AC-17(2), AC-18(1)
SV-AC-3	Compromised master keys or any encryption key	x						The operator cyber plan should protect the encryption keys from disclosure using a robust key management strategy in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	IA-5, IA-5(7), IA-7, SC-12, SC-12(1), SC-12(2), SC-12(3), SC-13, SC-28(1)
SV-AC-8	Malicious use of hardware commands - backdoors / critical commands	x						The operator should ensure all hardware/backdoor commands available for use by the SV are appropriate.	SI-10, SI-10(3)
SV-AV-1	Communications system jamming resulting in denial of service and loss of availability and data integrity			x				The SV should be resilient against communications and positioning jamming attempts.	CP-8, AC-18(5), SC-5, SC-40, SC-40(1), SC-40(3), SI-10, SI-10(3)
SV-IT-1	Communications system spoofing resulting in denial of service and loss of availability and data integrity	x		x				The SV should be resilient against communications and positioning spoofing attempts.	AU-8(1), CP-8, SC-5, SC-40, SC-40(1), SC-40(3), SI-10, SI-10(3)

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-MA-3	Attacks on critical software subsystems (e.g., Attitude Determination and Control (AD&C), Telemetry, Tracking and Commanding (TT&C), Command and Data Handling (C&DH), and Electrical Power Subsystem (EPS))					x		The SV should protect mission critical subsystems by ensuring their confidentiality, integrity, and availability are protected during SV operations.	SI-10, SI-10(3), SI-17, CP-12, SC-3
SV-MA-7	Exploit ground system and use the system to maliciously to interact with the SV				x	x		The Program should prevent unauthorized access to the SV from the ground segment.	Should have controls from many control families, here are the most important: AC - Access Control AU - Audit and Accountability CM - Configuration Management CP - Contingency Planning IA - Identification and Authentication IR - Incident Response MP - Media Protection PE - Physical and Environmental Protection RA - Risk Assessment CA - Security Assessment and Authorization SC - System and Communications Protection SI - System and Information Integrity SA - System and Services Acquisition

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-SP-1	Exploitation of software vulnerabilities (bugs); Unsecure code, logic errors, etc. in the FSW					x	x	The Program should perform software assurance of internally developed and acquired software that includes use of established robust procedures and technical methods.	CA-8, CM-3(2), CM-4(1), CM-5(3), RA-5, RA-5(1), RA-5(2), SA-10, SA-11, SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(7), SA-11(8), SA-15, SA-15(4), SA-15(5), SA-15(7), SA-15(8), SA-3, SA-4(3), SA-4(5), SI-2, SI-2(6), SI-7(14)
SV-AC-7	Weak communication protocols - those without strong encryption within them	x		x				The Program should only use acceptable secure communication protocols in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.	SA-4(9), SC-8, SC-8(1), SC-8(2), SC-8(3), SI-7(6)
SV-AV-5	Using fault management system against you: understanding the fault response could be leveraged to put the S/C in a vulnerable state. For example, safe-mode with crypto bypass, orbit correction maneuvers, affecting integrity of TLM to cause action from ground, or some sort of Rendezvous and Proximity Operation (RPO) to cause S/C to go into safe mode					x		The Program should protect all fault management documents (i.e. FMEA/FMECA artifacts) from inadvertent and inappropriate disclosure.	CP-10, CP-10(4), CP-12, IR-4, IR-4(3), SA-5, SC-24, SI-11, SI-17
SV-MA-5	Not being able to recover from cyber attack					x		The SV should recover to normal operations from a cyber-safe mode with executable fault management actions.	CP-2(5), IR-4

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-SP-3	Introduction of malicious software such as a virus, worm, Distributed Denial-Of-Service (DDOS) agent, keylogger, rootkit, or Trojan Horse					x	x	The Program should perform supply chain risk management of all SV software to include using established robust procedures and technical methods.	CA-8, CM-2(2) ,CM-3(2), CM-4(1), CM-5(3), CP-2(8), PL-8(2), RA-5, RA-5(1), RA-5(2), SA-10, SA-11, SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(7), SA-11(8), SA-12, SA-12(1), SA-12(11), SA-12(2), SA-12(5), SA-12(8), SA-12(9), SA-14, SA-15(3), SA-15(7), SA-19, SA-3, SA-4(3), SA-4(5), SC-38, SI-2, SI-7(14)
SV-SP-5	Hardware failure (i.e. tainted hardware) with a focus on application-specific integrated circuit (ASIC) and field programmable gate array (FGPA)					x	x	The Program should establish robust procedures and technical methods to prevent the introduction of tainted ASIC and FPGAs into the SV supply chain.	SA-12, SA-12(1)
SV-AC-2	Replay of recorded authentic communications traffic at a later time with the hope that the authorized communications will provide data or some other system reaction	x		x				The SV should prevent previously issued commands from reuse within the systems (i.e. replay attacks).	AU-3(1), IA-2(8), IA-2(9), IA-3, IA-3(1), IA-4, IA-7, SC-13, SC-23, SC-7, SC-7(11), SC-7(18), SI-3(9), SI-10, SI-10(5), AC-17(1), AC-17(2)
SV-MA-4	Not knowing what your crown jewels (i.e. operations or data that is most important to the accomplishment of critical missions) are and how to protect them now and in the future.					x		The Program should ensure all mission critical elements (hardware and software) comply with high levels of assurance for confidentiality, integrity, and availability to meet mission objectives.	CA-8,CP-2(8),RA-3,SA-12,SA-12(8), SA-14,SA-15(3),SC-7

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-SP-6	Software reuse, commercial off-the-shelf (COTS) dependence, and standardization of onboard systems using building block approach with addition of open source technology leads to supply chain threat					x	x	The Program should ensure reused, COTS, or open-source software meets mission needs and receives or has received adequate software assurance previously.	CA-8, CM-3(2) ,CM-4(1), CM-5(3), RA-5, RA-5(1), RA-5(2), SA-10, SA-11, SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(7), SA-11(8), SA-15, SA-15(4), SA-15(5), SA-15(7), SA-15(8), SI-2, SI-7(14)
SV-AC-6	Three main parts of S/C; the CPU, memory, and I/O interfaces with parallel and/or serial ports, are connected via busses (i.e. 1553) and need to be segregated.					x		The SV should employ segregation and least privilege principles for the on-board architecture, communications, and control.	AC-4, AC-4(14), AC-4(2), AC-6, SC-3, SC-4, SC-6, SC-7(21), SC-39, SI-17
SV-AV-6	Complete compromise or corruption of running state					x		The SV should provide the capability to enter the SV into a cyber-safe mode when cyber-attacks have been detected.	CP-10, CP-10(4), CP-12, IR-4, IR-4(3), SC-24, SI-11, SI-17
SV-SP-11	Software defined radio (SDR) is also another computer, networked to other parts of the SV that could be pivoted to by an attacker and infected with malicious code. Once access to an SDR is gained, the attacker could actually alter what the SDR thinks are correct frequencies and settings to communicate with the ground.	x		x				The Program should ensure Software Defined Radios are deemed critical to operations and supply chain risk management strategies are employed for both the hardware and software.	AC-3(2), CA-8, CM-3(2), CM-4(1), CP-2(8), PL-8(2), RA-5, RA-5(1), RA-5(2), SA-10, SA-11, SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(7), SA-11(8), SA-12, SA-12(1), SA-12(11), SA-12(2), SA-12(5), SA-12(8), SA-12(9), SA-15, SA-15(4), SA-15(5), SA-15(7), SA-15(8), SA-19, SC-38, SI-2, SI-7(14)

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-SP-4	General supply chain interruption or manipulation					x	x	The Program should protect against supply chain threats to the SV by employing security safeguards.	CP-2(8), PL-8(2), SA-11(5), SA-12, SA-12(1), SA-12(11), SA-12(2), SA-12(5), SA-12(8), SA-12(9), SA-14, SA-15(3), SA-19, SC-38
SV-CF-1	Tapping of communications links (wireline, RF, network) resulting in loss of confidentiality; traffic analysis to determine which entities are communicating with each other without being able to read the communicated information	x		x				The SV should protect communication links from loss in confidentiality.	AC-3(10), SC-7(18), IA-7, SC-13
SV-AV-4	Attacking the scheduling table to affect tasking					x		The SV should ensure any update to task scheduling functionality has met high assurance standards before execution.	AC-3(2)
SV-IT-4	Cause bit flip on memory via single event upsets					x		The SV should leverage high availability and a memory integrity solution to protect against single event upsets.	SI-16
SV-MA-6	Not planning for security on SV or designing in security from the beginning					x		The Program should specifically develop a defense-in-depth architecture for the SV and document within applicable security documentation.	PL-2, PL-2(3), PL-8, PL-8(1), SA-2, SA-8, SA-17

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-MA-8	Payload (or other component) is told to constantly sense, emit, or run a mission to the point that it drains the battery constantly / operates in a loop at maximum power until the battery is depleted.					x		The SV should implement protections to prevent components (i.e. payloads) from draining power from the SV.	SC-6
SV-SP-2	Testing only focuses on functional requirements and rarely considers end to end or abuse cases					x		The Program should establish robust procedures and technical methods to perform testing to include negative testing (i.e. abuse cases) of the SV hardware and software.	CA-8, RA-5, RA-5(1), RA-5(2), SA-11, SA-11(1), SA-11(2), SA-11(5), SA-11(7), SA-11(8), SA-15(7), SA-3, SA-4(3)
SV-SP-7	Software can be broken down into three levels (operating system and drivers layer, data handling service layer, and the application layer). Highest impact on the system is likely the embedded code at the BIOS, kernel/firmware level or attacking the on-board operating systems.					x	x	The Program should ensure the SV's operating systems are scrutinized/whitelisted and have received adequate software assurance previously.	CA-8, CM-3(2), CM-4(1), CM-7(5), RA-5, RA-5(1), RA-5(2), SA-10, SA-11, SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(7), SA-11(8), SA-15, SA-15(4), SA-15(5), SA-15(7), SA-15(8), SA-4(5), SI-2, SI-7(14)

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-SP-9	On-orbit software updates/upgrades/patches/direct memory writes. If the TT&C, Mission Operations Center (MOC), or even the developer's environment is compromised, risk exists for a variation of a supply chain attack where malicious code is injected after the s/c is in orbit					x	x	The SV software updates shall be validated for integrity and functionality prior to deployment.	AC-3(2), CA-8, CM-3(2), CM-4(1), CM-5(3), RA-5, RA-5(1), RA-5(2), SA-10, SA-11, SA-11(1), SA-11(2), SA-11(4), SA-11(5), SA-11(6), SA-11(7), SA-11(8), SA-15, SA-15(4), SA-15(5), SA-15(7), SA-15(8), SA-3, SA-4(3), SA-4(5), SI-2, SI-2(6), SI-7(14)
SV-CF-3	Knowledge of target satellite's cyber-related design details would be crucial to inform potential attacker - so threat is leaking of design data which is often stored unclassified or on contractor's network					x		The Program should define and protect Essential Elements of Information (EEI) from unauthorized disclosure.	SA-5

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-DCO-1	Not knowing that you were attacked or attack was attempted					x		The SV should detect on-board intrusions. The SV should prevent on-board intrusions. The SV should audit and log on-board information assurance events. When the SV has detected an intrusion on-board, the SV should send an alert and onboard cyber information to the mission ground station within [mission-appropriate timelines minutes]. When the SV has prevented an intrusion on-board, the SV should send an alert and onboard cyber information to the mission ground station within [mission-appropriate timelines minutes].	AU-2, AU-3, AU-3(1), AU-4, AU-4(1), AU-5, AU-5(2), AU-6(1), AU-6(4), AU-8, AU-9, AU-9(2), AU-9(3), AU-14, SI-4, SI-4(2), SI-4(4), SI-4(10), SI-4(16), SI-4(5), SI-6, SI-7(8), SI-16, IR-4, IR-5, IR-5(1), SC-5(3), SC-7(9), SI-17, SI-4(11)
SV-IT-2 (ties to SV-AV-5)	Unauthorized modification or corruption of data	x		x		x		The SV should protect the confidentiality and integrity of all information at all times (i.e. transmission, preparation, storage, etc.).	SI-7, SI-7(1), SI-7(2), SI-7(5), SI-7(8), SA-10(1), SC-8, SC-8(2), SC-28, SC-28(1), SI-7(6)
SV-SP-10	Compromise development environment source code (applicable to development environments not covered by threat SV-SP-1, SV-SP-3 and SV-SP-4).					x	x	The Program should ensure security requirements/configurations are placed on the development environments to prevent the compromise of source code from supply chain or information leakage perspective.	SA-15

TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-AV-2	Satellites base many operations on timing especially since many operations are automated. Cyber attack to disrupt timing/timers could affect the SV (Time Jamming / Time Spoofing)					x		The SV should protect the integrity and availability of the authoritative time source.	
SV-AV-3	Affect the watchdog timer onboard the satellite which could force satellite into some sort of recovery mode/protocol					x		The Program should perform in-depth analysis of watchdog timer implementation to achieve high levels of assurance that the implementation will satisfy mission objections and that the availability and integrity is protected.	
SV-AV-7	The TT&C is the lead contributor to satellite failure over the first 10 years on-orbit, around 20% of the time. The failures due to gyro are around 12% between year one and six on-orbit and then ramp up starting around year six and overtake the contributions of the TT&C subsystem to satellite failure. Need to ensure equipment is not counterfeit and the supply chain is sound.	x						The Program should apply risk mitigation strategies to reduce the threat of TT&C failing over time.	CP-10, CP-10(4), CP-12, CP-2(8), IR-4, IR-4(3), SA-11(5), SA-12, SA-12(1), SA-12(11), SA-12(2), SA-12(5), SA-12(8), SA-12(9), SA-14, SA-15(3), SA-19, SC-24, SC-3, SC-38, SI-10, SI-10(3), SI-11, SI-17
SV-IT-3	Compromise boot memory					x		The SV should establish a root of trust on the boot process for the flight software.	SI-7(9)

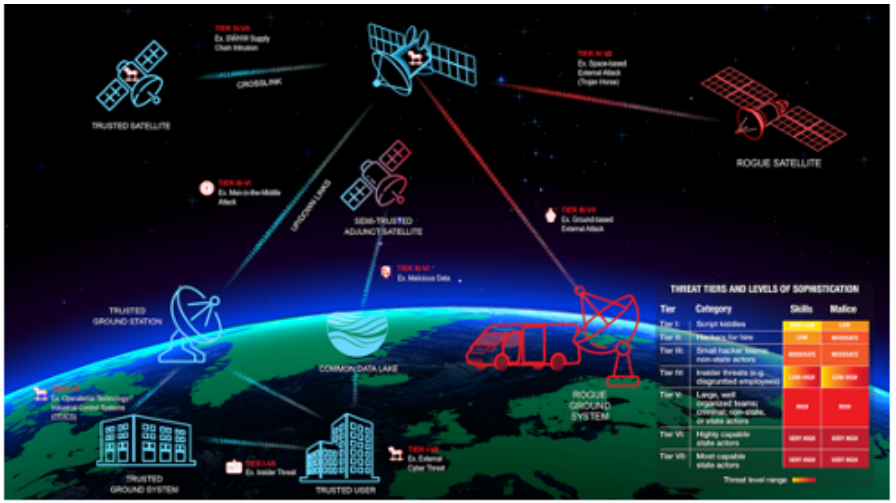
TOR 2021-01333 Threat ID	Threat/Vulnerability High Level Description	Relevant SPD-5 Principles						High Level Best Practices	NIST Controls To Help Mitigate
		SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)		
SV-AC-4	Masquerading as an authorized entity in order to gain access/insider threat		x			x		The Program should establish policy and procedures to prevent individuals (i.e. insiders) from masquerading as individuals with valid access to areas where commanding of the SV is possible.	AT-2(2), IR-4(7), PE-3, PM-12, PS-4
SV-CF-4	Adversary monitors for safe-mode indicators such that they know when satellite is in weakened state and then they launch attack					x		The SV should protect the confidentiality and integrity of all information at all times (i.e. transmission, preparation, storage, etc.).	SC-8, SC-13
SV-IT-5	Onboard control procedures (i.e. ATS/RTS) that execute a scripts/sets of commands					x	x	The SV should ensure any update to on-board stored procedures has met high assurance standards before execution.	AC-3(2)
SV-AC-5	Proximity operations (i.e. grappling satellite)		x					The Program should disable any maintenance and development access to the SV before launch (i.e. JTAG ports)	SC-41
SV-MA-2	Heaters and flow valves of the propulsion subsystem are controlled by electric signals so cyber attacks against these signals could cause propellant lines to freeze, lock valves, waste propellant or even put in de-orbit or unstable spinning			x				The SV should protect mission critical subsystems from electric signal interference.	PE-19, PE-19(1)
SV-CF-2	Eavesdropping (RF and proximity)					x		The SV should eliminate and then mitigate information leakage due to electromagnetic signals emanations.	AC-3(10), IA-7, PE-19, PE-19(1), SC-7(18), SC-13, SC-28, SC-28(1), SI-7(6)

Threats Grouped by SPD-5 Principles

Filter by Threat Levels

SPD-5 (i)	SPD-5 (ii)	SPD-5 (iii)	SPD-5 (iv)	SPD-5 (v)	SPD-5 (vi)
SV-AC-1	SV-AC-1	SV-AV-1	SV-MA-7	SV-MA-3	SV-SP-1
SV-AC-3	SV-AC-4	SV-IT-1		SV-MA-7	SV-SP-3
SV-AC-8	SV-AC-5	SV-AC-7		SV-SP-1	SV-SP-5
SV-IT-1		SV-AC-2		SV-AV-5	SV-SP-6
SV-AC-7		SV-SP-11		SV-MA-5	SV-SP-4
SV-AC-2		SV-CF-1		SV-SP-3	SV-SP-7
SV-SP-11		SV-IT-2		SV-SP-5	SV-SP-9
SV-CF-1		SV-MA-2		SV-MA-4	SV-SP-10
SV-IT-2				SV-SP-6	SV-IT-5
SV-AV-7				SV-AC-6	
				SV-AV-6	
				SV-SP-4	
				SV-AV-4	
				SV-IT-4	
				SV-MA-6	
				SV-MA-8	
				SV-SP-2	
				SV-SP-7	
				SV-SP-9	
				SV-CF-3	
				SV-DCO-1	
				SV-IT-2	
				SV-SP-10	
				SV-AV-2	
				SV-AV-3	
				SV-IT-3	
				SV-AC-4	
				SV-CF-4	
				SV-IT-5	
				SV-CF-2	

Threat Tier
I
II
III
IV
V
VI & VII



Tier	Name	Skills	Maliciousness	Motivation	Methods
I	Script Kiddies	Very low	Low	Boredom, thrill seeking	Download and run already-written hacking scripts known as "toolkits"
II	Hackers for Hire	Low	Moderate	Prestige, personal gain, thrill seeking	Write own scripts, engage in malicious acts, brag about exploits
III	Small Hacker Teams, Non-State Actors OR Disorganized/Non-Advanced State Actors	Moderate	Moderate	Power, prestige, intellectual gain, respect	Write scripts and automated tools
IV	Insider Threats (e.g., disgruntled employees)	Very Low – Very High	Very Low – Very High	Unwitting, ideology, politics, espionage	Insider knowledge lowers the barrier of entry. Methods span the spectrum from simple to sophisticated.
V	Large, Well-Organized Teams, Criminal, Non-State, or State Actors	High	High	Personal gain, greed, revenge	Sophisticated attacks by criminal/thieves, may be "guns for hire" or involved in organized crime
VI	Highly-Capable State Actors	Very high	Very high	Ideology, politics, espionage	State sponsored, well-funded cyber-attacks against enemy nations
VII	Most Capable State Actors				

Appendix B
Questionnaire on Understanding Cybersecurity Risks and Gaps for a Space System

The below questionnaire provides approximately 40 questions you may want to consider when understanding cyber risks/gaps for a space system. Commercial providers providing space systems / services may find it useful to answer these questions to gain insight into their approaches for mitigating cyber risk.

The below table consists of three columns:

- Question – the question the applicant should answer
- Further Detail – amplified details to provide contextual information on the question
- Label / Category – a method to group the types of questions being asked. Below are the categories of questions being asked:
    - Secure Design / Planning: ensuring adequate security engineering is occurring for the system
    - Risk Assessment: ensuring appropriate assessments are being performed
    - Communication Security: is proper security being applied to ensure confidentiality, integrity, and availability is being protected on communication links
    - Configuration Management: ensuring proper change management procedures are in place
    - Development Environment: ensuring protecting of development environment so malicious actors cannot inject malicious software into codebase
    - Input Validation: ensuring proper testing and input sanitization is occurring
    - Insider Threat: ensuing insider threat is considered and appropriately mitigated
    - Interconnections: ensuring any interconnection between space system and externals is properly documented and the risk is understood
    - Least Functionality: ensuring only the required features of a system are configured.
    - Least Privilege/ Segmentation: ensuring adequate permissions are engineered into the system with least access/privilege being the default approach
    - Monitoring: ensuring proper monitoring across the entire environment is occurring to include the space vehicle
    - Secure Boot: ensuring root of trust is established to protect the integrity of the software loading process
    - Software Assurance: ensuring software is adequately tested and functions properly
    - Supply Chain Risk Management: ensuring protections are in place for both hardware and software supply chains

Question	Further Detail	Label/Category
What cybersecurity standard do you currently leverage for development, launch, and operations of the space system?	For example, NIST 800-53, NIST 800-171/172, CMMC, SOX, PCI, etc.	secure design / planning
Do you have program-specific security assessment and authorization policies and procedures (i.e. ATOs) and do they apply to both the space vehicle and ground?	Many security standards have a validation or certification step. What steps are taken to ensure the security controls and standards are being met?	risk assessment
If your space vehicle has commanding capability, how are you protecting the commanding capability from intrusion?	For example authenticated encryption could be used. Ideally NIST- or NSA-compliant implementation (i.e., FIPS 140-2), for a range of security protocols (e.g., the encryptor/decryptor implementation, key generation, key management, key distribution, testing, and pre- and post-launch physical security).	communication security
If your space vehicle has commanding capability, how are you resilient against communications and positioning jamming attempts?	Signal jamming has been used for decades against space systems by adversaries and thought by many as the leading threat against a space system. For example, are multiple uplink paths in use? Is the space system utilizing Transmision Security (TRANSEC)? TRANSEC is used to ensure the availability of transmissions and limit intelligence collection from the transmissions. TRANSEC is secured through burst encoding, frequency hopping, or spread spectrum methods where the required pseudorandom sequence generation is controlled by a cryptographic algorithm and key. Such keys are known as transmission security keys (TSK). The objectives of transmission security are low probability of interception (LPI), low probability of detection (LPD), and antijam which means resistance to jamming (EPM or ECCM). Additionally, the ground system maintains the ability to establish communication with the space vehicle in the event of an anomaly to the primary receive path. Receiver communication can be established after an anomaly with such capabilities as multiple receive apertures, redundant paths within receivers, redundant receivers, fallback default command modes, and lower bit rates for contingency communication, as examples.	communication security

If your space vehicle has commanding capability, how are you resilient against communications and positioning spoofing attempts?	Ideally the space system incorporates backup sources for navigation and timing. For example, fault-tolerant authoritative position and time sourcing that leverage voting schemes that include inputs from backup sources. Consider providing a second reference frame against which short-term changes or interferences can be compared. The space should internally monitor GPS performance so that changes or interruptions in the navigation or timing are flagged. Leveraging strong cryptographic mechanisms can help achieve adequate protection against the effects of intentional electromagnetic interference.	communication security
Have hardware (backdoor) commands that could adversely affect mission success if used maliciously been identified and evaluated?	Confirm that only hardware commands for the purpose of providing emergency access are being used, and that commanding authority is appropriately restricted, eliminating as many such unnecessary commands as is practical. Test commands not needed for flight should be deleted or disabled.	communication security
Are/How are you protecting encryption keys from disclosure and are you using a robust key management strategy in accordance with industry standards like CNSSP 12, NIST, or CCSDS Key Management?	FIPS-compliant technology used should include (but is not limited to) cryptographic key generation algorithms or key distribution techniques that are either a) specified in a FIPS, or b) adopted in a FIPS and specified either in an appendix to the FIPS or in a document referenced by the FIPS. For systems requiring NSA encryption, NSA-approved technology used for symmetric key management by the Program should include (but is not limited to) NSA-approved cryptographic algorithms, cryptographic key generation algorithms or key distribution techniques, authentication techniques, or evaluation criteria.	communication security
Are/How are you protecting communication links from loss in confidentiality?	If commanding of the space system is enabled, the space system should not employ a mode of operations where cryptography on the commanding link can be disabled (i.e., crypto-bypass mode). The space system should implement cryptography for the indicated uses using the indicated protocols, algorithms, and mechanisms, in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards. For example, NSA-certified or approved cryptography for protection of classified information, FIPS-validated cryptography for the provision of hashing.	communication security

Are/How are you preventing previously issued commands from reuse within the systems (i.e., replay attacks)?	The space system should implement relay and replay-resistant authentication mechanisms for establishing a remote connection. The space system should uniquely identify and authenticate the ground station before establishing any connection. Authenticating the ground station (and all commands) before establishing remote connections using bidirectional authentication that is cryptographically based is a best practice. This can include embedding opcodes in command strings, using trusted authentication protocols, identifying proper link characteristics such as emitter location, expected range of receive power, expected modulation, data rates, communication protocols, beamwidth, etc.; and tracking command counter increments against expected values.	communication security
Are/How are you protecting confidentiality and integrity of all information at all times (i.e., transmission, preparation, storage, etc.)?	Encryption should be used at times. Storage (i.e., data-at-rest) and transmission. Where needed, integrity validation of data should be performed.	communication security
Do you have program-specific configuration management policies and procedures for the hardware and software for the ground and space vehicle?	Configuration change controls for organizational information systems involve the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers, and mobile devices), unscheduled/unauthorized changes, and changes to remediate vulnerabilities. The developers/maintainers develop the initial installation build and each release build, which needs to have a clearly documented baseline configuration. For the developer/integrator, the emphasis is on the development and document aspects, but they also need to maintain the information on that baseline configuration as part of the developer CM system. Maintaining baseline configurations requires creating new baselines as organizational information systems change over time. Baseline configurations of information systems must reflect the current enterprise architecture. The developer/maintainer must maintain those configurations under configuration control, prohibiting any unauthorized changes to the baseline configuration.	configuration management

Are/How are you ensuring security requirements/configurations are placed on the development environments to prevent the compromise of source code from supply chain or information leakage perspective?	The development environment is often overlooked as an attack vector for adversaries and is often a soft target. Likely one of the easiest methods to perform supply chain injection. Attacking the development environment and injecting malicious code has many examples of success: **SolarWinds** (https://www.zdnet.com/article/Microsoft-FireEye-confirm-SolarWinds-supply-chain-attack/) **CCleaner** (https://www.zdnet.com/article/avast-no-plans-to-discontinue-ccleaner-following-second-hack-in-two-years/) **NodeJS** (https://www.mandiant.com/resources/supply-chain-node-js)	development environment
Are/How are you protecting all fault management documents (i.e., FMEA/FMECA artifacts) from inadvertent and inappropriate disclosure?	Fault protection documents which are typically produced during system engineering (i.e., http://virtual-digital.com/fmea-a-systems-engineering-framework-for-cross-functional-validation#:~:text=FMEA%3A%20A%20Systems%20Engineering%20Framework%20for%20Cross%2DFunctional%20Validation,-Lionel%20Grealou%202020&text=Failure%20Mode%20and%20Effects%20Analysis,identify%20mitigation%20or%20resolution%20measures.) can provide a road map for attackers. The fault trees will identify items that can ultimately cause failure within a system and these documents must be protected. The faults management analysis process often identifies single points of failure which ultimately could be considered a vulnerability by security minded personnel. In the governmental sense, fault documents should be considered controlled unclassified information (CUI).	development environment
Is the system protected, any segment and any source, from improper or invalid input?	Primary focus is on the system command path, critical dependencies (e.g., PNT), and logic supporting key performance parameters. Consider internal and external system boundaries. Input errors can be due to command errors, bit flips in the channel, software errors, etc. Errors can also be due to deliberate manipulation or spoofing. Timing of input signals, if varied in an unexpected manner, may also trigger undesirable effects in the system. Test for good software hygiene, including assessment of software security controls, code analysis, and ongoing vulnerability scanning. Test plans should include deliberately malformed data input, including representative edge cases. Apply whitelists for valid data ranges when possible.	input validation

Are/How are you preventing individuals (i.e., insiders) from masquerading as individuals with valid access to areas where commanding of platform is possible (i.e., what is the insider threat strategy)?	An insider is any person who has or had authorized access to or knowledge of an organization's resources, including personnel, facilities, information, equipment, networks, and systems. Insider threat is the potential for an insider to use their authorized access or understanding of an organization to harm that organization. This harm can include malicious, complacent, or unintentional acts that negatively affect the integrity, confidentiality, and availability of the organization, its data, personnel, or facilities. The insider threat can be either unintentional or intentional. **Unintentional Threat** **Negligence** – An insider of this type exposes an organization to a threat through carelessness. Negligent insiders are generally familiar with security and/or IT policies but choose to ignore them, creating risk for the organization. Examples include allowing someone to "piggyback" through a secure entrance point, misplacing or losing a portable storage device containing sensitive information, and ignoring messages to install new updates and security patches. A**ccidental** – An insider of this type mistakenly causes an unintended risk to an organization. Organizations can successfully work to minimize accidents, but they will occur; they cannot be completely prevented, but those that occur can be mitigated. Examples include mistyping an email address and accidentally sending a sensitive business document to a competitor, unknowingly or inadvertently clicking on a hyperlink, opening an attachment that contains a virus within a phishing email, or improperly disposing of sensitive documents. **Intentional Threats** – Intentional threats are actions taken to harm an organization for personal benefit or to act on a personal grievance. The intentional insider is often synonymously referenced as a "malicious insider." The motivation is personal gain or harming the organization. For example, many insiders are motivated to "get even" due to unmet expectations related to a lack of recognition (e.g., promotion, bonuses, desirable travel) or even termination. Their actions include leaking sensitive information, harassing associates, sabotaging equipment, or perpetrating violence. Others have stolen proprietary data or intellectual property in the false hope of advancing their careers. **Other Threats** **Collusive Threats** – A subset of malicious insider threats is collusive threats, where one or more insiders collaborate with an external threat actor to compromise an organization. These incidents frequently involve cybercriminals recruiting an insider or several insiders to enable fraud, intellectual property theft, espionage, or a combination of the three. **Third-Party Threats** – Additionally, third-party threats are typically contractors or vendors who are not formal members of an organization, but who have been granted some level of	insider threat

	access to facilities, systems, networks, or people to complete their work. These threats may be direct or indirect threats. Direct threats are individuals who act in a way that compromises the targeted organization. Indirect threats are generally flaws in systems that expose resources to unintentional or malicious threat actors. Source: https://www.cisa.gov/defining-insider-threats	
Have all external partner and internal agency network interconnections and data flows to/from the project boundary been documented and assessed to assure a commensurate protection level of information being processed?	Ensure inherent risk to space systems as well as risk to mission data are understood, documented, and approved. For the purpose of mission assurance, ensure all interconnections coming from outside of the project have appropriate network segmentation. Ensure external partners and supporting systems processing sensitive data have adequate protections in place. At a minimum, these protections are documented in Interconnection Security Agreements that reference the implemented security controls allocated to that interface. Interconnections include individual remote connections (RDP, VPN, etc.). The project boundary encompasses all assets under direct project control. Protections for interconnections include multi-factor authentication, least privilege-based access controls, network segmentation, secure remote access protocols, and managed interconnections.	interconnections
Intentionally Left Blank		
Has least functionality been enacted across the mission? Are/How are you ensuring least functionality principles are in place for the space vehicle architecture, communications, and control as well as the ground environment?	The principle of least functionality provides that the space system is configured to provide only essential capabilities and to prohibit or restrict the use of non-essential functions, such as ports, protocols, and/or services that are not integral to the operation of that space system. For example, when using a Linux container, ensure only the required libraries/components are installed that are necessary for operations. Similarly using network/host firewalls to only allow required traffic. Also, on the space vehicle, when building the operating system, only include the required features of the operating system.	least functionality
Has least access required for each role been enacted across the mission? Are/How are you employing segregation and least privilege principles for the space vehicle architecture, communications, and control as well as the ground environment?	Limit access (authentication and authorization) to systems, resources and data to only that required for the role. Detect and respond to insider threats and unauthorized elevated privileges. Limit adverse consequences in the event of network penetration. Use a risk-based approach to implement access controls (e.g., two-factor PIV authentication or other IAL3/AAL3 credential) commensurate with mission needs.	least privilege / segmentation

Does the ground system architecture incorporate network segmentation and isolation as appropriate?	Identify the ground components that will be communicating and the data flows of this communication as well as specifics such as method/protocol and port/address. Ensure communications are isolated to only the components that need to communicate with one another.	least privilege / segmentation
Does the space vehicle system architecture incorporate adequate protections at the interfaces between components and subsystems to limit propagation of anomalous conditions?	Identify the flight components that will be communicating and the data flows of this communication as well as specifics such as method/protocol. Ensure communications are isolated to only the components that need to communicate with one another.	least privilege / segmentation
Are there telemetry monitoring capabilities on the ground or onboard to detect any unexpected conditions?	Unexpected conditions can include RF lock-ups, loss of lock, failure to acquire an expected contact and unexpected reports of acquisition, failure to acquire GPS satellites, unusual AGC and ACS control excursions, unusual navigation or timing behavior, unforeseen actuator powering or actions, thermal stresses, power aberrations, failure to authenticate, software or counter resets, etc. Mitigation might include additional telemetry monitor flags, specific AGC and PLL thresholds to alert operators, auto-capturing state snapshot images in memory when unexpected conditions occur, signal spectra measurements, and expanded default diagnostic telemetry modes to help in identifying and resolving anomalous conditions.	monitoring
Are there procedures being incorporated into the CONOPS to log/report “suspicious” anomalies (e.g., tripped telemetry monitors, aberrant science) if unresolved, or if unexplained artifacts are discovered in post-processed (e.g., science and housekeeping) trending data?	Also need to identify specific criteria for "suspicious" (potentially malicious) anomalies and unexplained excursions in post-processed mission data, and generate procedures for timely reporting. Evolve the criteria during flight to minimize false positives.	monitoring
Are/How are you performing intrusion detection, intrusion prevention, and auditing/logging capability on-board the space vehicle that can alert and downlink onboard cyber information to the mission ground station?	Monitoring on the space vehicle for cyber indicators of compromise is often overlooked as necessary but it should not be. Monitoring "at the edge" is important as it is the ultimate ground truth when detecting malicious activity within the space system. Monitoring the information systems on the ground is equally important but the combination of vehicle monitoring with ground system monitoring provides the most robust solution from a monitoring perspective.	monitoring

Do you have program-specific incident response policies for the space vehicle and ground?	Monitoring is a prerequisite to response, but monitoring without response action is futile especially with a space system. Policies must include response actions for when indicators of compromise are identified which must extend from ground to space vehicle.	monitoring
Has an end-to-end risk assessment been performed for the entire mission thread and network interconnections? **[Applies to both Space and Ground Systems] - What are your program-specific risk assessment policies to include both the space vehicle and ground?**	Select critical mission threads for analysis. Identify supporting infrastructure and associated security controls. Include elements outside direct project control if the mission depends on these elements. Identify known vulnerabilities associated with the mission. Characterize feasible attacks. Assess the likelihood and potential impact of successful exploits. Propose mitigations to address the risks. This process should be done on a continual basis. Cyber risks from all elements of the end-to-end architecture should be evaluated on a continuous basis throughout the project lifecycle, including during operations. Recommend that projects conduct risk assessments in accordance with NIST guidance (NIST publications contain risk assessment guidance beyond sole vulnerability assessments) and to integrate cyber risks into project risk management.	risk assessment
Are/How are you establishing a root of trust on the boot process for the space vehicle software?	It is important for the computing module to be able to access a set of functions and commands that it trusts; that is, that it knows to be true. This concept is referred to as root of trust (RoT) and should be included in the design. With RoT, a device can always be trusted to operate as expected. RoT functions, such as verifying the device's own code and configuration, must be implemented in secure hardware (i.e., field programmable gate arrays). By checking the security of each stage of power-up, RoT devices form the first link in a chain of trust that protects the space vehicle.	secure boot
Has failure analyses addressed maliciously induced effects across the mission architecture, assessing Ground, and Space segment fault, risk, and failure modes?	The mission-specific threats can be used to generate an assessment of how the overall architecture would react to each threat and what the indicators would be. Consider if new system-level risks are identified by the aggregation of heritage and newly developed system characteristics. The assessments should be coordinated with the appropriate stakeholders: for example implementation and I&T organizations, scientists, operators, etc., to ensure the indicator(s) will be identified as a threat response, and reported correctly.	secure design / planning

Has the program/project considered how it will demonstrate the ability to promptly detect, report, mitigate, and recover from unauthorized activity within the operations/space center(s) and essential mission information flows?	Maintain sufficient awareness of normal operations, network, and IT system performance so that anomalous behavior or unauthorized activity can be rapidly identified and managed. Unauthorized activity is a subset of malicious activity such as a network intrusion. The program/project should identify its essential operations processes and systems. For the identified elements, ensure that a sufficient transaction history is stored for trending and historical analysis, a capability to monitor for signs of unauthorized activity is in place and tested, and alerts are relayed to appropriate parties for review and action. Essential operations processes may include command load generation, ground system configuration management (e.g., updates/changes), and cryptographic key management. Essential systems may include the operations physical access control, console operator authentication/logon/ logoff records, network interfaces to the operations areas, and associated internal IT services. Program/project should work with the various appropriate cybersecurity teams to a common understanding on identifying anomalous or unauthorized activity, sharing/relaying of data including alerts, and testing to ensure capabilities are functioning as intended.	secure design / planning
Are/How are you preventing unauthorized access to the space vehicle from the ground segment?	The ground as a method to attack the space vehicle is often thought to be the most likely cyberattack vector. The ground segment must be secured accordingly, explain what controls/standards/etc. are in place on the ground system to reduce the risk of attack against the vehicle. Are all interactions from the ground to the SV being monitored for malicious activity?	secure design / planning
Are/How are you developing a defense-in-depth architecture for the space system (i.e., space vehicle and ground) and document within applicable security documentation?	One strategy to ensure the end-to-end system is secure is leveraging defense-in-depth. Is the system leveraging these principles in the security strategy?	secure design / planning
Are/How are you protecting the integrity and availability of the authoritative time source?	Timing on real-time embedded systems is crucial. What steps are being taken to ensure timing is accurate? For example, were voting schemes adopted (i.e., triple modular redundancy) that include inputs from backup sources. Was a second reference frame considered for which short-term changes or interferences can be compared?	secure design / planning
Are/How are you leveraging high availability and integrity memory solution to protect from single event upsets?	Space vehicles operate under stress and may be exposed to high radiation thereby requiring high integrity solutions for memory as single event upsets can occur. What protections are in place to protect memory from these single event upsets?	secure design / planning

Are/How are you performing software assurance of internally developed and acquired software to include using established robust procedures and technical methods?	While there are various methodologies related to security testing software, if you boil down the technical side of the methodologies there are six technical areas that appear in the methodologies. Typically, software risk can come in three areas of weakness in the code that may be exploited (coding errors or design flaws), known vulnerabilities to attack (unpatched or misconfigured software), or using libraries that have known vulnerabilities which is often a function of the previous two items. The technical analysis methods associated with software security assurance can typically be broken down into six major technical analysis approaches to reduce exposure to risks and vulnerabilities. ● Static Application Security Testing: Analysis of the source code for exposure to CWEs, adherence to good practices, and standards and analysis of code complexity ● Vulnerability / Hardening Analysis: Vulnerability analysis identifies CVEs and assess compliance against ● Dynamic Analysis: Dynamic testing attempts to break into the software (fuzz/penetration testing) ● Binary Analysis: Analysis of the binary code for exposure to CWEs, adherence to good practices, and standards and analysis of code complexity. This can be performed without source code access (i.e., commercial software / third party software) ● Origin Analysis / Software Composition Analysis: Identify CVE exposure and risk with open-source licenses. This can be performed without source code access (i.e., commercial software / third party software) ● Software Bill of Materials (SBOM): Generation of SBOM based on the aforementioned composition/origin analysis and cross referencing to vulnerability databases to understand the decomposition of software and inherit known vulnerabilities/risk. SBOM are more accurate if generated from a Whitebox perspective (i.e., with source code) but can also be partially generated from a Blackbox perspective (i.e., without source code)	software assurance
Are software updates validated for integrity (i.e., digital signing/certs) and functionality prior to deployment?	Are multiple checks to be performed prior to executing software updates? Are digital signatures or hash or CRC or a checksum being used to validate integrity on software updates on the ground and space vehicles?	software assurance

Are/How are you assuring reused software meets mission needs and receives or has received adequate software assurance previously?	In mission systems, like space systems, software reuse is often high due to the reliability factor. However, as threats have evolved and new testing methods are identified, reused software may contain vulnerabilities that have never been discovered. When reusing software it is imperative to confirm its heritage from a software assurance and testing perspective and fill any gaps that may be present with the software assurance approach. Rescanning/testing code should be performed regardless as new vulnerabilities are disclosed daily.	software assurance
Are/How are you ensuring the space vehicle's operating system is scrutinized and has received adequate software assurance currently or previously?	Similar to reused software, the operating system must receive adequate software assurance. Many engineers will assume the operating system is "secure" due to its prevalence of use in the community. However, Linux Kernels, Windows Operating Systems, VxWorks, etc. all continue to have critical vulnerabilities disclosed year after year. Therefore, it is imperative due diligence is performed with respect to the operating system as these are common attack vectors for adversaries.	software assurance
Are/How are you ensuring robust procedures and technical methods are used to perform testing to include negative testing (i.e., abuse cases) of the platform hardware and software?	When performing verification and validation, adequate abuse cases should be considered. According to OWASP (https://cheatsheetseries.owasp.org/cheatsheets/Abuse_Case_Cheat_Sheet.html), an Abuse Case can be defined as a way to use a feature that was not expected by the implementer, allowing an attacker to influence the feature or outcome of use of the feature based on the attacker action (or input). Negative testing using abuse cases is critical when building a testing approach. Testing should assure the software/system does what it is supposed to do, does not do what it is not supposed to do, and that the software/system operates properly under adverse conditions. Often engineers only test the nominal paths within the system, but negative/abuse case testing is a must to ensure robustness.	software assurance
Are/How are you ensuring any update to on-board software, memory, or stored procedures has met high assurance standards before execution?	Space vehicles operate with autonomy, especially the flight termination system, and therefore must be engineered with high assurance of working. When performing any update to the system prior to launch, what assurance methods/tests are performed to ensure the updates do not interject risk into the system. These updates are also a vector for adversaries to inject backdoors, trojans, time-bombs, etc. The high assurance standard should account for not only coding flaws but potential malicious code injections by an adversary/insider.	software assurance

Are/How are you performing supply chain risk management of all hardware and platform software to include using established robust procedures and technical methods?	For hardware/software that is not being developed in-house (i.e., outsourced), consider what assurance is being performed prior or during integration. On the software side, some form of the previously mentioned six technical analysis methods should be performed. ● **Static Application Security Testing**: Analysis of the source code for exposure to CWEs, adherence to good practices, and standards and analysis of code complexity ● **Vulnerability/Hardening Analysis**: Vulnerability analysis identifies CVEs and assess compliance against ● **Dynamic Analysis**: Dynamic testing attempts to break into the software (fuzz/penetration testing) ● **Binary Analysis**: Analysis of the binary code for exposure to CWEs, adherence to good practices, and standards and analysis of code complexity. This can be performed without source code access (i.e., commercial software / third party software) ● **Origin Analysis / Software Composition Analysis**: Identify CVE exposure and risk with open-source licenses. This can be performed without source code access (i.e., commercial software / third party software) ● **Software Bill of Materials (SBOM)**: Generation of SBOM based on the aforementioned composition/origin analysis and cross referencing to vulnerability databases to understand the decomposition of software and inherit known vulnerabilities/risk. SBOM are more accurate if generated from a Whitebox perspective (i.e., with source code) but can also be partially generated from a Blackbox perspective (i.e., without source code)	supply chain risk management
Are/How are you ensuring robust procedures and technical methods to prevent the introduction of tainted ASIC and FPGAs into the platform supply chain?	ASIC/FPGA, if being used, is often forgotten in the supply chain discussion. Are trusted foundries being used? What verification and validation is being performed before acceptance and integration? Malicious logic can be embedded during fabrication similar to injecting software into the development environments (i.e., SolarWinds attack) and this must be considered before integrating the ASIC/FPGA into the space vehicle.	supply chain risk management

Appendix C

Overview of Department of Defense and National Aeronautics and Space Administration Cybersecurity Policy Documents

This appendix serves as a reference to existing cybersecurity policy documents created by the Department of Defense (DoD) and National Aeronautics and Space Administration (NASA) that may be relevant for CRSRA applicants or licensees.

1.0 DoD Acquisition Documents Relating to Cybersecurity

For space systems performing DoD missions, the DoD family of documents on cybersecurity appear in the Committee on National Security Systems (CNSS) library. For commercial systems used for DoD missions the overarching policy document is:

- **CNSSP 12** *Cybersecurity Policy for Space Systems Used to Support National Security Missions*[32]

There are many supporting documents addressing topics from encryption to managing insider threats. The supporting documents also include:

- **CNSSI 1200** *Instruction for Space Systems Used to Support NSS*[33]

2.0 NASA Space Protection Documents

NASA also has developed space protection guidelines that are applicable to NASA programs after 2020. NASA STD-1006, titled "Space System Protection Standard," focuses mostly on the satellite's security; however, NASA has a long-standing cybersecurity approach for the ground and launch systems which are governed by FIPS PUB 199 and the NIST Risk Management Framework. NASA created the 2810 series of NASA Policy Directives and NASA Procedural Requirements that leverage FIPS and NIST as the guiding principles from which guidance was derived. For more information on the NASA Space System Protection Standard see:

- **NASA STD-1006** *Space System Protection Standard*
  - Description: https://www.nasa.gov/sites/default/files/atoms/files/nasa-mrpp-space-protection-requirements-20201118.pdf
  - Document: https://standards.nasa.gov/standard/NASA/NASA-STD-1006

[32] Cybersecurity Policy for Space Systems Used to Support National Security MIssions (CNSSP) 12 (Feb. 2018), Link: https://www.cnss.gov/CNSS/openDoc.cfm?l8QxUU6Sk+qSHuYioX7Tyg==.

[33] Cybersecurity Policy for Space Systems Used to Support National Security MIssions (CNSSP) 1200 (May 2014), Link: https://www.cnss.gov/CNSS/openDoc.cfm?Pimn0EB3vwC2wA4Czi/kjg==