FAQs for Protecting SMD Spaceborne Assets

13 May 2020

Command Uplink Encryption

Q: Why is this requirement coming out now?
A: Space is highly contested. There are many malicious actors who would take great pride in controlling or doing damage to a NASA asset. There is also concrete evidence of malicious attempts to gain control of NASA spacecraft.

Q: Are any missions excluded from implementing encryption capability?
A: The requirement for command uplink encryption applies to missions with the following exceptions, however, all missions should ensure the integrity of their command link.

- Hosted instrument payloads
- Class C or D spacecraft without a propulsion subsystem
- Spacecraft designed to operate beyond 2M km

Even missions falling under these exceptions should consider whether adding encryption would be prudent. While ensuring command integrity may not include encryption, there should, at a minimum, be a level of authentication included. For hosted payloads, in particular, these projects should maintain command authority up to the point where the commands are handed over to the host. All exceptions are subject to change at the discretion of senior leadership or if new threats arise.

Q: Does this apply to Announcements of Opportunity (AOs)?
A: YES. New language has been added to the standard AOs to require this capability be included in the proposal.

Q: Do current missions (in development) have to implement this requirement?
A: Missions currently in development should assess the benefit of implementing encryption against the impact to cost and schedule to determine whether they should add encryption to their mission. This assessment should be provided to NASA management for concurrence.

Q: Does this apply to partner spacecraft?
A: If communications with the spacecraft is the responsibility of the partner, then NO, this requirement does not apply to them. However, NASA should engage in conversation with our partners to encourage them to be prudent in the security of their spacecraft.

If NASA is providing the communications capability for the spacecraft, then YES, this requirement applies.

Q: Does this apply to reimbursable missions?
A: NASA does not levy our requirements on reimbursable missions. However, NASA should engage in conversation with our partners to encourage them to be prudent in the security of their spacecraft.

Q: Does this apply to technology demonstration projects?
A: YES. The requirement for command uplink encryption applies unless the project falls under one of the approved exceptions (again with the recommendation of using command authentication):

- Hosted instrument payloads
- Class C or D spacecraft without a propulsion subsystem
- Spacecraft designed to operate beyond 2M km

Q: Does this requirement replace the Candidate Protection Strategies as used in developing a Project Protection Plan?
A: This requirement is a formalization of the related questions addressed in the Candidate Protection Strategies. The Project Protection Plan will address how the project is implementing this requirement.

Q: For the exclusion for 'spacecraft designed to operate beyond 2M km,' how do you address the timeframe while the mission is in transit (and still in Earth orbit)?
A: If the mission is only in Earth orbit for a brief period of time until it transits deeper into space, then encryption is not currently required, but authentication should be implemented. This also applies to missions performing an Earth fly-by.

Q: There is an exclusion for 'Class C or D spacecraft without a propulsion subsystem' but what if there is a command sent which causes the battery to discharge (resulting in an explosive event)? Wouldn't this seem to indicate there should be no exclusions?
A: At this time, such a scenario is considered very unlikely, therefore this exclusion is appropriate. If future analyses determine there are threats against this type of mission which would warrant inclusion of command uplink encryption, the exclusion will be re-examined.

Q: FIPS 140 comes in a variety of levels. Which level is required? Is there flexibility in this requirement?
A: Level 1 implementation is the minimum. Projects are requested to investigate implementing at Level 2. Higher levels of protection are advantageous, within the cost constraints of the project.

Q: Is AES (FIPS 197) allowed?
A: YES. This is documented in FIPS 140 as a valid algorithm to use for Symmetric Key Encryption and Decryption and Message Authentication. Note FIPS 197 describes the algorithm whereas FIPS 140 describes how the specific implementation is verified and validated, including the algorithm. Compliance with FIPS 197 does not, in and of itself, imply compliance with FIPS 140. However, it is a good first step. The project would need to ensure its implementation of FIPS 197 has been validated under the FIPS 140 process.

Q: What is the process to implement this requirement in the on-board computer for spacecraft?
A: Commercial software or hardware is available to implement command encryption/decryption. Additionally, GSFC and JPL have implemented this requirement in current missions which software may be available to other projects (within ITAR and other constraints).

Q: What is the cost estimate to implement this requirement?
A: Cost estimates depend on the level of encryption being implemented and from which vendor the project obtains the hardware and/or software.

Q: Where do I go for more details on how to implement this requirement?
A: FIPS 140 standards are described at https://www.nist.gov/itl/current-fips .
Currently available COTS software and hardware can be found via Internet searches on this topic, and the FIPS 140 document contains a link to their system validation page, including which modules, hardware, or software have been formally validated.

Q: Does command uplink encryption have an implication to the SCaN tracking assets (SN, NEN, DSN)?
A: NO. There are currently no identified impacts to SCaN assets.

Q: What qualifies as a propulsion system? Does an Attitude Control System count?
A: The intention is to prevent missions being turned into a threat to other nearby missions. Therefore, any system that can change the orbital parameters of a spacecraft could be considered 'propulsion'. The fundamental concern is the time it would take for an operator to recognize the mission is acting suspiciously and intervene. Under normal conditions, the operator would not react instantaneously, therefore, command encryption would be recommended.

Q: When developing an initial design for command encryption, is it necessary to have access to classified threat information?
A: NO. Access to classified threat information is not necessary to begin an assessment of the appropriate implementation of command encryption. Designers should review current, publicly available information for initial assessments and consider additional questions. For example, are there potential adversaries already operating in the orbital regime in which the mission will operate? Have there been attacks on similar missions? Is any of the technology used on the mission of particular interest to adversaries? Teams are recommended to review:
'Competing in Space', NASIC, January 2019
(https://www.nasic.af.mil/Portals/19/documents/Space_Glossy_FINAL--15Jan_Single_Page.pdf?ver=2019-01-23-150035-697) or
'Challenges to Security in Space', DIA, February 2019
(https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf)

Q: Have formal NASA requirements been developed regarding command encryption?
A: YES. NASA-STD-1006 has been developed which codifies requirements for command encryption, surviving PNT interference, and protecting command data as Sensitive But Unclassified (SBU) (among other topics). This standard was formally approved by the NASA Chief Engineer in October 2019.

Q: Does this apply to lunar landers?
A: YES. NASA-STD-1006, signed in October 2019, codifies that missions at lunar distances need to implement command encryption.

Q: Should only current threats be considered when designing to mitigate threats?
A: NO. When designing the mission, not only should current threats be considered (classified or unclassified), project teams should consider how the threat environment is evolving. Given our flight projects last for many years, the design isn't only for what the threat environment looks like during the design phase; it should consider what the threat environment could look like during the entire lifetime of the mission. Mission Resilience and Protection Program (MRPP) personnel can assist in understanding the broad picture of the threat environment.

Q: How will the project implementation of encryption be verified?
A: The project should include verification of this implementation as part of their integration and test process. In other words, there should be specific tests included to verify this requirement just as there would be for any other requirement on the project.

Q: Does the project's solution for encryption need to be independently FIPS certified or can FIPS compliance be verified by the project itself?
A: FIPS compliance of their encryption solution may be verified by the project. They do not need to pay for a separate, independent certification. On the other hand, for the project to verify their solution is FIPS compliant, they can point to the FIPS web site listing of compliant systems. Those systems will have been independently certified, so the end result is the same.

Recognizing and Surviving Position, Navigation, and Timing (PNT) Interference

Q: Why is this requirement coming out now?
A: Space is highly contested. There are many malicious actors who would take great pride in controlling or doing damage to a NASA asset. There is also concrete evidence of malicious attempts to interfere with GPS signals.

Q: Are any missions excluded from implementing an alternate PNT capability?
A: There are no exclusions from addressing alternatives for PNT capabilities.

Q: Does this apply to Announcements of Opportunity (AOs)?
A: YES. New language has been added to the standard AOs to require this capability be included in the proposal.

Q: Do current missions (in development) have to implement this requirement?
A: Missions currently in development should assess the benefit of implementing additional PNT solutions against the impact to cost and schedule to determine whether they should add this capability to their mission.

Q: Does this apply to partner spacecraft?
A: If PNT is the responsibility of the partner, then NO, this requirement does not apply to them. However, NASA should engage in conversation with our partners to encourage them to be prudent in ensuring the integrity and accuracy of their spacecraft position, navigation, and timing.

If NASA is providing the PNT capability for the spacecraft, then YES, this requirement applies.

Q: Does this apply to reimbursable missions?
A: NASA does not levy our requirements on reimbursable missions. However, NASA should engage in conversation with our partners to encourage them to be prudent in ensuring the integrity and accuracy of their spacecraft position, navigation, and timing.

Q: Does this requirement replace the Candidate Protection Strategies as used in developing a Project Protection Plan?
A: This requirement is a formalization of the related questions addressed in the Candidate Protection Strategies. The Project Protection Plan will address how the project is implementing this requirement.

Q: This requirement appears to only relate to GPS. If the spacecraft doesn't use GPS (such as hosted payloads or spacecraft going beyond the Moon), does this requirement still apply?
A: While the initial intent was protection for projects using GPS, any mission for which PNT accuracy is critical should examine whether a backup capability for their planned PNT implementation would be prudent.

Q: Is the intent of the requirement to 'detect' interference as opposed to 'recognize' it? Note: a 'PNT Subsystem' would include elements such as wheels and torquers which would be designed to neither 'detect' nor 'recognize' interference.
A: YES. The intent is to detect interference and take appropriate action which would include safeguarding the spacecraft, instruments, and data, and reporting the interference to MRPP and management personnel as appropriate.

Q: Is the intent of the requirement to 'monitor' for intrusions or interference (either on-board or on the ground)?
A: YES. Missions should detect and monitor telemetry for intrusions or interference and take appropriate action. This can take place either on-board or on the ground, at the discretion of the project.

Q: What are the recommended ways to detect interference with the GPS data?
A: There are no formal recommendations at this time, however, some PNT filtering algorithms that blend high-fidelity models of orbital dynamics and/or a diversity of measurement sources have been proven in flight operations to detect and survive interference. NASA/TP-2018-219822, *Navigation Filter Best Practices,* describes NASA best practices for navigation filter design.

Q: Have formal NASA requirements been developed regarding surviving PNT interference?
A: YES. NASA-STD-1006 has been developed which codifies requirements for command encryption, surviving PNT interference, and protecting command data as SBU (among other topics). This standard was formally approved by the NASA Chief Engineer in October 2019.

Q: How would an operator know if there were PNT interference occurring?
A: There are two parts of an answer for this question: 1) the mission should be designed such that the appropriate telemetry information is available to the operators to suggest an interference or inappropriate action is occurring and 2) the operations staff should be trained to recognize a telemetry response which could potentially mean an inappropriate action is occurring. When operations personnel see an unexplained interference, they should notify Mission Resilience and Protection Program (MRPP) personnel.

Protecting Command Uplink Information as Sensitive But Unclassified (SBU)

Q: Why is this requirement coming out now?
A: Space is highly contested. There are many malicious actors who would take great pride in controlling or doing damage to a NASA asset. There is also concrete evidence of malicious attempts to exfiltrate NASA mission information.

Q: Does this apply to all missions, regardless of the current phase of the project?
A: YES. This requirement applies to all missions.

Q: Does this apply to Announcements of Opportunity (AOs)?
A: YES. New language has been added to the standard AOs to require this capability be included in the proposal.

Q: Does this apply to partner spacecraft?
A: YES. All command information should be protected, regardless of the system on which it resides. This may entail negotiation with the partners regarding the definition and protection strategies of SBU data.

Q: Does this apply to reimbursable missions?
A: NASA does not levy our requirements on reimbursable missions. However, NASA should engage in conversation with our partners to encourage them to be prudent in the security of information related to their spacecraft.

Q: Does this requirement replace the Candidate Protection Strategies as in developing a Project Protection Plan?
A: This requirement is a formalization of the related questions addressed in the Candidate Protection Strategies. The Project Protection Plan will address how the project is implementing this requirement.

Q: What is the process for implementing this?
A: If the material is being shared via email, that email message should be encrypted. Encryption is also recommended for data-at-rest, but at a minimum, the data should be labeled as SBU, and handled accordingly. This data should never be posted on a public Web site.

Q: How broadly should this requirement for 'information' protection be interpreted? For example, if a presentation package mentions there will be command encryption but does not give the details which would expose vulnerabilities, does that presentation package need to be labeled as SBU? Please clarify.
A: If the protection implementation details are described in the document, that document (whether it be Word, PDF, PowerPoint, or some other format) should be labeled and handled as SBU. If the wording in the document states there will be protection but does not contain the details of the implementation, that document does not need to be labeled as SBU. When in doubt, consult with local Mission Resilience and Protection Program (MRPP) or Security personnel.

Q: Have formal NASA requirements been developed protecting command data as SBU?
A: YES. NASA-STD-1006 has been developed which codifies requirements for command encryption, surviving PNT interference, and protecting command data as SBU (among other topics). This standard was formally approved by the NASA Chief Engineer in October 2019.

Interference Reporting

Q: What should an operator do if they see any unexplained interference?
A: Operators should report any unexplained interference (whether with PNT or commands or any other system) to Mission Resilience and Protection Program (MRPP) personnel. The MRPP

team can assist with determining whether the interference was purposeful and to assist with mitigation strategies.

Q: How will an operator know if they are seeing malicious interference?
A: Operators should be trained to recognize telemetry responses which are unusual. It is not up to the operator to determine whether that response is due to an adversary, they are just to report the incident to MRPP personnel. There should also be regular proficiency training; the recommended frequency is annual.