Before the

**FEDERAL COMMUNICATIONS COMMISSION**

Washington, DC 20554

|  |  |
| --- | --- |
| In the Matter of )  )  Mitigation of Orbital Debris in the New Space Age ) | IB Docket No. 18-313 |

**COMMENTS OF PROVIDENCE ACCESS COMPANY**

Providence Access Company (“Providence”)[[1]](#footnote-1) respectfully submits these comments in response to the Federal Communications Commission’s (the “Commission”) Notice of Proposed Rulemaking in the above-captioned proceeding.[[2]](#footnote-2) Providence advises satellite and associated network operators on cybersecurity requirements and best practices and its founder and Chief Executive Officer serves as the U.S. industry lead for the joint NSA/Defense Information Systems Agency’s (DISA) Commercial Space INFOSEC Working Group (CSIWG).[[3]](#footnote-3)

**I. A CONTROLLED ORBITAL ENVIRONMENT IS CRITICAL FOR THE SUCCESS OF THE COMMERCIAL SPACE INDUSTRY AND THE NATION**

Providence commends the Commission for initiating this proceeding to keep space safe as the number of space users and applications grows and the environment becomes even more congested, contested, and competitive.[[4]](#footnote-4) Providence limits its comments to the Commission’s proposals in the NPRM that would add a requirement for a Commission space station licensee to protect its satellite command uplinks and telemetry downlinks using encryption and expects that other commenters will address other aspects of the Commission’s NPRM.[[5]](#footnote-5)

In order to control the orbital environment, it is clear that satellite operators must take responsible measures to ensure that they, and only they, can remotely command their satellites to maneuver and communicate. Unauthorized commands sent to a satellite could cause changes to its location and velocity and/or alter its communications payload(s), increasing the possibility it would cause harmful interference to other systems or even become involved in a collision with other satellites or orbital debris. An on-orbit collision with another satellite or orbital debris could, depending on the objects and relative velocities involved, result in long-lived space debris that could degrade or even make infeasible the use of certain orbits. The satellite operators and their authorizing nations, including the United States itself, would likely suffer irreparable reputational damage and, in the case of operators authorized by the FCC, become embroiled in extended discussions of U.S. liability under the Outer Space Treaty, the Liability Convention, and other laws.[[6]](#footnote-6) It is essential the entire space community work together to prevent any collisions, and ensuring positive control of satellite command systems is an important part of an overall approach to space safety and sustainability.

**II. SATELLITES ARE SUBJECT TO CYBERSECURITY RISKS INCLUDING COMMAND INTRUSION**

Unfortunately, the fact that satellites are located in space does not make them immune from attempts to interfere with their operation. The United States Department of Defense and the Intelligence Community closely monitor threats to satellite systems, including civil and commercial systems. The National Air and Space Intelligence Center (NASIC), a highly-regarded center of expertise on space threats and trends recently released an unclassified report, “Competing in Space” covering trends, challenges, and threats to U.S. and allied use of space.[[7]](#footnote-7) NASIC notes that “[s]atellite command and data distribution networks expose space systems, ground infrastructure, users, and the links connecting these segments to cyber threats.



The graphic [above] indicates possible cyber threats to each of a space system’s segments.”[[8]](#footnote-8)

As the unclassified NASIC Report shows, U.S. Government experts are concerned about threats of Command Intrusion, Payload Control, and Denial of Service to the Space Segment.[[9]](#footnote-9)

Even more than a decade ago there were reports of potential satellite space segment hack attempts to two NGSO satellites (Terra AM-1 and LANDSAT-7).[[10]](#footnote-10) In 2014 China allegedly compromised the systems and data products of the NOAA National Weather Service satellites at four sites, reportedly through compromise of the ground systems.[[11]](#footnote-11) Private sector security experts suggest that “historically, the engineers behind satellites and their communications structures have been governed by the principle of safety – but only recently, information security has started making its way onto designers’ radars.”[[12]](#footnote-12) Other satellites may have been targeted or even compromised, but satellite operators typically do not publicly discuss their specific operations or cybersecurity posture.

Clearly, no defense is impenetrable but making no attempt at defense is unconscionable. In today’s cyber environment it is clear that securing the command and telemetry links of satellites from unauthorized remote commands is an important consideration of an overall security program design. Encryption is widely used to protect access to network control devices, computers, and to secure information in transit across the Internet; satellites can and do use encryption, too.[[13]](#footnote-13) Providence believes that embarking on a new satellite program without carefully considering security issues designed to ensure the satellite operator maintains positive control of its system is reckless.

**III. THE COMMISSION’S PROPOSED RULE FOR ENCRYPTION SHOULD BE CLARIFIED BECAUSE DESIGNING AND IMPLEMENTING CRYPTOGRAPHY WELL IS VERY DIFFICULT**

The Commission proposes to adopt the following new Part 25.290 rule:

“*For space stations that include onboard propulsion systems, operators must encrypt telemetry, tracking, and command communications with the space station.*”[[14]](#footnote-14)

The Commission’s rule is properly limited to those space stations that if compromised could be improperly commanded to alter their orbits, posing a higher degree of collision risk or, presumably, of being maneuvered outside their coordinated orbits where their continued operation and radio-frequency (RF) emissions could cause harmful interference to other satellites. This encryption required rule would appear to be even more important for NGSO satellites that may not be continuously tracked, commanded, and monitored as they orbit.[[15]](#footnote-15) However, the Commission’s proposed rule does not go far enough: it does not specify what kinds of encryption are sufficient to meet the rule or contain other security design objective.[[16]](#footnote-16)

Bruce Schneier, a recognized world-class expert in applied cryptography, has noted that developing cryptographic systems is very difficult, error prone, and that secure systems tend to re-use well-established, studied, and heritage cryptographic designs, algorithms, and implementations.[[17]](#footnote-17) Applicants for space station licenses or other FCC approval may be tempted to implement their own encryption solutions to meet the plain text of the Commission’s otherwise sensible rule. As other security professionals have noted, “When one sets out to reinvent the wheel, one takes upon themselves the risk of reinventing the wheel *poorly*.”[[18]](#footnote-18) It is essential that *effectively implemented cryptographic solutions* be used on satellites, not simply “encryption” as the Commission proposes.[[19]](#footnote-19) Fortunately, there is an expert U.S. Government agency that has a long process heritage of working with commercial space companies to ensure their satellites use rigorously evaluated encryption algorithms and implementations to maintain positive control of satellites throughout their lifetime: the National Security Agency.

**IV. THE UNITED STATES HAS REQUIRED ALL GOVERNMENT AND COMMERCIAL FOREIGN AND DOMESTIC SATELLITES SUPPORTING NATIONAL SECURITY TO PROTECT THEIR COMMAND UPLINK USING NSA-APPROVED COMMERCIAL SOLUTIONS SINCE 2007 AND TELEMETRY SINCE 2012**

The U.S. Government’s Committee on National Security Systems (CNSS), to which the Commission appoints a non-voting observer, has issued policies that apply cryptography requirements to commercial satellites used for U.S. national security purposes.[[20]](#footnote-20) The relevant policy is CNSS Policy No. 12 (CNSSP-12), last revised in 2018, which applies to “. . . all space NSS that are developed, owned, operated, controlled, or leased either by the USG or for the benefit of the USG by commercial entities (domestic and foreign) or foreign governments under bilateral or multilateral agreements. . . “, and further provides in relevant part:

*16. The following cryptographic requirements must be addressed and satisfied:*

*a. NSA-approved cryptographies and cryptographic techniques, implementations, and associated security architectures, must be used wherever cryptography or cryptographic techniques are needed in applicable systems. At a minimum, they will be used to:*

*(1) Authenticate and end-to-end encrypt all system commands (e.g. space platform bus and all payload commands) transmitted over any communications link accessible by unauthorized personnel in accordance with their classification or sensitivity.*

*(2) End-to-end encrypt all data (e.g. space platform bus and payload command echoes, telemetry, health and status, mission data, and communications relay) transmitted over any communications link accessible by unauthorized personnel in accordance with their classification or sensitivity unless otherwise indicated below.*[[21]](#footnote-21)

The functional effect of CNSSP-12 is that many satellite operators, including those licensed by the FCC, already choose to use “NSA-approved cryptographies and cryptographic techniques, implementations, and associated security architectures” in their satellites and ground control systems rather than trying to create their own cryptography because they intend to provide services to the U.S. Government. This also ensures that effective cryptography is being used as, over time, older cipher algorithms and implementations are deprecated and ultimately decertified.[[22]](#footnote-22) A number of space-qualified and associated ground encryptors/decryptors are commercially available, NSA-approved, and ready for integration while others are being developed and evaluated.[[23]](#footnote-23)

**V. THE PROPOSED RULE ON ENCRYPTION SHOULD BE MODIFIED TO BETTER REFLECT ITS PURPOSE AND FACILITATE ADOPTION**

Admittedly, not all of the satellites licensed or otherwise authorized by the Commission for U.S. market entry will ever be considered “National Security Systems”. However, many will be. Providence proposes that the Commission modify its proposed rule to align with CNSSP-12, provide a means for applicants to demonstrate compliance, and reserve Commission flexibility to make determinations on the adequacy of specific cryptographic implementations on a case-by-case basis. Accordingly, Providence recommends the following modified rule:

§ 25.290 Telemetry and command encryption.

For space stations that include onboard propulsion systems, operators must secure telemetry and command communications with the space station using (a) an encryption solution for which the U.S. National Security Agency has issued an approval letter for its space stations pursuant to the Committee on National Security Space Systems Policy No. 12, or (b) provide details to the Commission demonstrating that its non-NSA approved solution will effectively protect the confidentiality, integrity, and availability of the space station command and telemetry links during operation by (i) authenticating and end-to-end encrypting all system commands (e.g. space platform bus and all payload commands) and (ii) end-to-end encrypting all telemetry data (e.g. space platform bus and payload command echoes, telemetry, and health and status).

Providence suggests that any references to “tracking” be removed from any rule as non-relevant to the goal of preventing creation of orbital debris or maintaining positive control of a satellite. If the Commission adopted this revised rule, applicants could routinely satisfy it by (i) using the well-established processes to obtain and present a CNSSP-12 approval letter from the NSA, (ii) building their own effective solution (subject to Commission review and public notice), or (iii) requesting a waiver. This rule should apply to all space station applicants and those non-U.S. licensed space station operators over whom the Commission must make a U.S. market access determination.[[24]](#footnote-24)

**VI. CONCLUSION**

As space becomes more congested, contested, and competitive it is more important than ever that all satellite operators, including those who are subject to Commission jurisdiction, maintain positive control of their spacecraft. Encryption is one important security approach: ensuring that only authorized commands are received and processed by a given satellite contributes to its positive control; encrypting its telemetry adds a further layer of security against potential satellite attacks. Securing the command and telemetry channels using NSA-approved encryption has long been mandatory for U.S. and non-U.S. commercial satellites used to support the U.S. Government’s own requirements and is routinely used by many responsible satellite operators. Because designing and implementing effective encryption systems is very hard to do, the Commission should carefully examine any claims by operators that do not employ NSA-evaluated and approved cryptography implementations, and its proposed rule should be modified to reflect the need for effective cryptography to promote positive control of space stations throughout their entire mission lifecycle.

Respectfully submitted,

**PROVIDENCE ACCESS COMPANY**

By: /s/ *Andrew R. D’Uva*

Andrew R. D’Uva

President and Chief Executive Officer

Providence Access Company

2111 Wilson Boulevard, Suite 700

Arlington, Virginia 22201

(202) 621-2167

April 5, 2019

1. For more information on PAC, see [www.providence-access.com](http://www.providence-access.com). [↑](#footnote-ref-1)
2. *Mitigation of Orbital Debris in the New Space Age*, Notice of Proposed Rulemaking and Order on Reconsideration, IB Dkt No. 18-313, FCC 18-159 (rel. Nov. 19, 2018) (“NPRM”). [↑](#footnote-ref-2)
3. The views expressed here are those of Providence and do not reflect an official CSIWG position. [↑](#footnote-ref-3)
4. *See generally* NPRM. [↑](#footnote-ref-4)
5. NPRM at ¶ 75 and Appendix A. The Commission has long considered whether its space station applicants are legally, financially, and technically qualified to become licensees; Providence considers it well within the Commission’s authority to determine the sufficiency of the technical means proposed to support positive satellite control, such as the presence of effective encryption systems to secure command and telemetry links, falls squarely into the Commission’s established legal authority and decades of regulatory practice. [↑](#footnote-ref-5)
6. *See generally*, Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (“OST”), 18 UST 2410, 610 UNTS 205, 6 ILM 386 (1967); Convention on International Liability for Damage Caused by Space Objects (“Liability Convention”), 961 UNTS 187; 24 UST 2389; 10 ILM 965 (1971). Generally, under the OST and the Liability Convention the launching State is financially responsible for the acts of its authorized non-State (i.e., commercial) satellite operators. *See also* NPRM at ¶¶ 76 – 81. [↑](#footnote-ref-6)
7. “Competing in Space”, National Air and Space Intelligence Center (January 16, 2019), available at <https://media.defense.gov/2019/Jan/16/2002080386/-1/-1/1/190115-F-NV711-0002.PDF> (“NASIC Report”). [↑](#footnote-ref-7)
8. NASIC Report at 15. [↑](#footnote-ref-8)
9. See also “Challenges to Security in Space”, U.S. Defense Intelligence Agency (January, 2019). Available at <https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space\_Threat\_V14\_020119\_sm.pdf> [↑](#footnote-ref-9)
10. Wolf, Jim. “China key suspect in U.S. satellite hacks: commission” Reuters (2011). Available at < https://www.reuters.com/article/us-china-usa-satellite-idUSTRE79R4O320111028> [↑](#footnote-ref-10)
11. Flaherty, M.P, Samenow, J., and Rein, L. “Chinese hack U.S. weather systems, satellite network” *Washington Post* (November 12, 2014). Available at <https://www.washingtonpost.com/local/chinese-hack-us-weather-systems-satellite-network/2014/11/12/bef1206a-68e9-11e4-b053-65cea7903f2e\_story.html> [↑](#footnote-ref-11)
12. O’Donnell, L. “RSA Conference 2019: The Sky’s the Limit for Satellite Hacks” *Threatpost* (March 6, 2019). Available at <https://threatpost.com/rsa-conference-2019-the-skys-the-limit-for-satellite-hacks/142541/> [↑](#footnote-ref-12)
13. One important Internet standard is the Transport Layer Security (TLS) Protocol 1.3 of the Internet Engineering Task Force, commonly known as RFC 8446. TLS is a protocol that uses asymmetric encryption to secure devices through a chain of trust (i.e., ultimately relying on one or more shared root certificate authorities). This is appropriate for the Internet of Things, but overly complex for most satellite applications. Today, typical satellite encryption products generally implement FIPS-197, the Advanced Encryption Standard, using pre-shared 256-bit Cipher Keys (i.e., the satellite owner loads keys into the spacecraft and ground control systems prior to launch). *See* https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.197.pdf [↑](#footnote-ref-13)
14. NPRM Appendix A at ¶ 9. [↑](#footnote-ref-14)
15. GSO satellite operators typically use an earth station to communicate continuously with the satellite’s command receiver, even when not actually sending the satellite commands. This prevents some attempts to transmit unauthorized commands via RF to the satellite as the command receiver is already locked to the signal from the operator ground station. In the case of NGSO systems it is quite foreseeable that an operator may design the satellites to be accessed from the ground command/telemetry station(s) periodically, rather than continuously – making it easier for an unauthorized user to transmit to the command receiver of the satellite, provided they can track its orbit and keep the earth station correctly oriented. [↑](#footnote-ref-15)
16. For example, the Commission could specify that the encryption must be reasonably designed to protect the confidentiality, integrity and availability of the satellite command and telemetry links. Typical security objectives include protecting the confidentiality, integrity, and availability of a system or the data it contains. Encryption provides confidentiality, properly designed and implemented cryptologic approaches can offer integrity, and availability can be engineered using a variety of cryptographic and other techniques (e.g., encoding to protect against bit errors). [↑](#footnote-ref-16)
17. Schneier, Bruce. "Cryptography: The importance of not being different." Computer 32.3 (1999): 108-109. Available at <https://www.schneier.com/essays/archives/1999/03/cryptography\_the\_imp.html> [↑](#footnote-ref-17)
18. Herzog, Ben and Balmas, Yaniv. “Great Crypto Failures.” Weblog (May 23, 2016): p. 5. Available at <https://blog.checkpoint.com/wp-content/uploads/2016/10/GreatCryptoFailuresWhitepaper\_Draft2.pdf> [↑](#footnote-ref-18)
19. Not all encryption is strong, and none remains strong forever; cryptosystems have a lifecycle. Systems like the M-94 used by the U.S. Army from 1923 – 1942 (an implementation of the Jefferson Disk wheel cipher) are prone to rapid “breaks” using modern cryptanalysis techniques and computers. *See* https://en.wikipedia.org/wiki/Jefferson\_disk. [↑](#footnote-ref-19)
20. CNSS “provides a forum for the discussion of policy issues and is responsible for setting national-level cybersecurity policies, directives, instructions, operational procedures, guidance and advisories for U.S. Government (USG) departments and agencies for the security of National Security Systems (NSS) through the CNSS Issuance System. The CNSS is directed to assure the security of NSS against technical exploitation by providing: reliable and continuing assessments of threats and vulnerabilities and implementation of effective countermeasures; a technical base within the USG to achieve this security; and support from the private sector to enhance that technical base assuring that information systems security products are available to secure NSS.” Available at <https://www.cnss.gov/CNSS/about/about.cfm> [↑](#footnote-ref-20)
21. Available at <https://www.cnss.gov/CNSS/issuances/Policies.cfm>. CNSSP-12 replaced NSTISSP-12 (2001) which required NSA-approved cryptography for domestic satellite operators to protect the satellite command uplinks, but not the telemetry. [↑](#footnote-ref-21)
22. For example, the NSA previously approved a command security solution called Caribou but since January 2015 longer issues new CNSSP-12 approval letters for new satellites which would use it, moving instead to implementations using AES-256. Information Assurance Advisory No IAA-007-2012 “(U//FOUO) National Security Agency (NSA) Position on the Use of the Advanced Encryption Standard (AES) for Space Systems”, November 15, 2012. [↑](#footnote-ref-22)
23. Space COMSEC products including those approved by NSA for commercial/civil use are available from multiple suppliers including L3 Technologies Inc., (https://www2.l3t.com/trf/products/space\_mission\_assurance.htm), Innoflight (https://www.innoflight.com/product-overview/modern-space-comsec/), and Raytheon (https://www.raytheon.com/capabilities/products/space\_encryption). [↑](#footnote-ref-23)
24. The NSA routinely provides CNSSP-12 approvals to non-U.S., non-FCC licensed satellite operators. [↑](#footnote-ref-24)