BEFORE THE
FEDERAL COMMUNICATIONS COMMISSION
Washington, D.C. 20554

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

COMMENTS OF CHARLES CLANCY AND JONATHAN BLACK

Dr. Charles Clancy is the Bradley Professor of Cybersecurity at Virginia Tech, where he serves as the executive director of the Hume Center for National Security and Technology, and interim executive director of the Commonwealth Cyber Initiative. He is an internationally-recognized expert in cybersecurity for telecommunications and wireless systems. Prior to joining Virginia Tech in 2010 he served as the engineering leader for emerging mobile technologies within Laboratory for Telecommunications Sciences at the National Security Agency. He received his PhD from the University of Maryland and is co-author to over 200 academic publications, six books, and over 20 patents. He is co-founder to four venture-backed startup companies, including HawkEye 360, which performs commercial space-based detection and geolocation of terrestrial wireless signals.

Dr. Jonathan Black is a Professor in the Kevin T. Crofton Department of Aerospace and Ocean Engineering at Virginia Tech (VT), the Director of the Aerospace and Ocean Systems Laboratory of the Hume Center for National Security and Technology, a member of the Center for Space Science and Engineering Research (Space@VT), and the Northrop Grumman Senior Faculty Fellow in C4ISR. Prior to joining VT, Dr. Black served as a faculty member in the Aeronautics and Astronautics department at the Air Force Institute of Technology (AFIT), Wright-Patterson Air Force Base, Ohio. There he was the founding Director of the Center for Space Research and Assurance.

COMMENTS

I. Background

In section III.F.3 of the rulemaking, paragraphs 74 and 75, the Commission seeks comment on "… encryption for telemetry, tracking, and command communications for satellites with propulsion capabilities, and propose to add a requirement to our operational rules ...", with a particular emphasis on the circumstances under which encryption should be required. Within these comments we seek to provide such recommendations.

II. CNSSP-12 Ecosystem

The Committee on National Security Systems Policy 12 (CNSSP-12) governs the encryption requirements for satellites that provide services to the US government. The policy has historically required that the Telemetry, Tracking, and Command (TT&C) links have NSA-approved encryption devices, algorithms, and keys. Updated requirements published in February 2018 include encryption of all data communications to and from satellites using "NSA-approved cryptographies and cryptographic techniques, implementations, and associated security architectures."

A key challenge is that there are very limited options for NSA-approved hardware. Fully integrated radios that include the approved encryption chips operate at much lower data rates; have a significant impact on size, weight, and power budgets for small spacecraft; and can be cost prohibitive for cubesat-scale projects. Additionally the required key management infrastructure may be familiar to a large defense contractor, but not small commercially-oriented space startup companies or universities.

Beyond the encryption requirement, CNSSP-12 has specific requirements around communications waveform security, cybersecurity risk management, and supply chain security. While these may be desirable best practices, requirements like application of Federal Information Security Management Act (FISMA) requirements from NIST Special Publication 800-53 may not be appropriate for a commercial satellite.

III. Recommendations

1. Cybersecurity for satellites must be considered end-to-end, within the context of a risk-based management framework (RBMF). This risk management must include not only the impact to the owner/operator of the satellite if it is compromised, but also how it may affect other satellites in orbit as a result being compromised. For example, hacked satellites with propulsion represent a greater risk to their on-orbit neighbors.

2. Small satellites, particularly those built and flown for commercial, academic, and/or scientific applications, have almost no guidance or regulation on cybersecurity or cyber resiliency. There is, therefore, a clear need to analyze, evaluate, establish, publish, and refine best-practices. A standing government working group consisting of government, Federally Funded Research and Development Center (FFRDC), academic, and corporate members is recommend, charged with compiling an RBMF. This framework should have different levels of requirements for the different spacecraft stakeholder communities (small/large, maneuverable/non-maneuverable, etc.). This approach will provide a level of assurance to the government as well as evaluations of the effectiveness of the framework and analyses and feedback of its costs. The Commission should tie spectrum licenses for satellites to submission and approval of cybersecurity management plans consistent with the established best practices.

3. We recommend against direct application of CNSSP-12 policies to all satellites. Even for certain classes of dual-use commercial satellites, CNSSP-12 is likely unachievable. NSA should develop guidelines under their Commercial Solutions for Classified (CSfC) program for satellites. Currently NSA publishes Capability Packages for a range of different connectivity technologies that allows for multiple layers of software encryption. If well-implemented software encryption was an option for meeting CNSSP-12 type requirements, many vendors who view the current hardware encryption requirements as unachievable would have a path toward both compliance and significant increased security.