June 25, 2020

Via E-Mail
Attn: Secure 5G RFC
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue
NW, Room 4725
Washington, DC 20230
secure5G@ntia.gov.

Re: Satellite Industry Association Comments in Docket No. 200521–0144

Dear Sir or Madam:

Introduction

The Satellite Industry Association (SIA) hereby provide their comments in the Secure 5G RFC proceeding referenced above (hereinafter, RFC).[1] SIA[2] is a U.S.-based trade association representing the leading satellite operators, manufacturers, launch providers, and ground equipment suppliers who serve commercial, civil, and military markets. The satellite industry has a long history of ensuring the security of its communications networks and equipment and therefore, fully supports the efforts of the Administration, the Department of Commerce (DOC) and the National Telecommunications and Information Administration (NTIA) in this area. Accordingly, SIA appreciates the opportunity to share its views on the development and deployment of a secure, reliable global 5G ecosystem, and how to improve U.S. leadership in 5G and beyond.

As NTIA is aware and as recognized by the White House,[3] satellite is an important part of the 5G ecosystem. It is extremely important that as the Administration develops policies and rules governing 5G to enable U.S. leadership and ensure the security of the network, that the important role that satellite plays be considered.

---

[1] *The National Strategy to Secure 5G Implementation Plan*, Request for Comment, Docket Number 200521-0144, National Telecommunications and Information Administration (May 28, 2020)

[2] SIA Executive Members include: Amazon; AT&T Services, Inc.; The Boeing Company; EchoStar Corporation; Intelsat S.A.; Iridium Communications Inc.; Kratos Defense & Security Solutions; Ligado Networks; Lockheed Martin Corporation; OneWeb; SES Americom, Inc.; Space Exploration Technologies Corp.; Spire Global Inc.; and Viasat Inc. SIA Associate Members include: ABS US Corp.; AIRBUS U.S. Space & Defense, Inc.; Amazon Web Services; Analytical Graphics, Inc.; Artel, LLC; Astranis Space Technologies Corp; Blue Origin; Eutelsat America Corp.; ExoAnalytic Solutions; Globalstar, Inc.; HawkEye 360; Hughes; Inmarsat, Inc.; Kymeta Corporation; Leonardo DRS; Lynk; Omnispace; OneWeb Satellites; Panasonic Avionics Corporation; Peraton; Planet; Telesat Canada; and XTAR, LLC. For more information on SIA, see www.sia.org.

[3] *Ensuring America Reaches its 5G Potential*, White House Office of Science and Technology Policy, 30 May 2019 https://www.whitehouse.gov/articles/ensuring-america-reaches-its-5g-potential/

SIA urges NTIA as it considers the best way to improve U.S. leadership in 5G and beyond to adhere to certain basic principles that have successfully guided the United States in the past. These include:

1) Utilizing a technology neutral approach in developing regulation including for the allocation of scarce resources such as spectrum and funding;
2) Eliminating unnecessary and burdensome regulation;
3) Creating an open, transparent and predictable regulatory regime;
4) Enabling globally harmonized spectrum and its long-term availability; and
5) Ensuing U.S. leadership and the support of U.S. industry in international forums the International Telecommunications Union.

These principles have been a guiding force in U.S. leadership in the past. By adhering to these principles in the 5G and beyond world, the United States government will help to enable the United States to take a leadership role in 5G.

SIA also supports the Administration's efforts to ensure a secure 5G ecosystem. Cybersecurity is critical to the deployment of 5G and is committed to enhancing satellite cybersecurity through both industry-driven best practices and implementation of cybersecurity standards. To that end, SIA and the Global VSAT Forum have agreed to a set of voluntary cyber security principles that are successfully guiding the way for the industry's approach to 5G.[4] These principles are:

1. ***Voluntary, industry-led efforts and public-private partnerships are the optimal way to address cybersecurity at the national or international levels.***
2. ***Satellite industry organizations should actively address cybersecurity using industry best practices for risk management.***
3. ***Robust cybersecurity is aided by voluntary information sharing, free from fear of adverse consequences.***

As NTIA and the U.S. government continue their efforts to ensure the security of the country's 5G networks, SIA welcomes the opportunity to work together through a multi-stakeholder approach, which includes the utilization of voluntary best practices. Working together the United States can achieve its goals in this area. Accordingly, SIA also welcomes NTIA's recent request for comment on promoting the sharing of supply chain risk information.[5]

SIA appreciates the opportunity to respond in this important proceeding. The satellite industry welcomes the opportunity to work with the United States government to ensure the continued leadership of the United States in 5G and the deployment of a secure, reliable 5G ecosystem in the United States and abroad.

[4] These are attached as []
[5] Add site.

Respectfully submitted,

/s/

SATELLITE INDUSTRY ASSOCIATION

Tom Stroup, President

1200 18th St., N.W., Suite 975

Washington, D.C. 20036

cc: Travis Hall

JOINT STATEMENT ON THE SATELLITE INDUSTRY'S COMMITMENT TO CYBERSECURITY

The Satellite Industry Association (SIA) and Global VSAT Forum (GVF) are leading trade associations representing the global satellite communications industry. SIA and GVF, on behalf of their members, issue this joint statement on the industry's commitment to cybersecurity.

Cybersecurity is critical to the satellite industry's core goal: providing mission critical, highly reliable, and secure connectivity. The satellite industry has a long history of providing secure solutions to diverse global customers, including military and government users, corporations of every size and type, the non-profit and scientific communities, and individual consumers. Drawing on the expertise of its diverse membership, and responding to the demands of its user community, the industry has become a leader in providing safe, reliable communications.

Given the reliance of our economy and national security on secure communications, evolving attacks by criminals, terrorists, and nation-states properly concern national leaders and the private sector. The cyber threat environment is complex, and the stakes are high. While no system can be perfectly secure, each organization's commitment to foundational security principles helps all contributors to the industry, from software vendors to equipment manufacturers and service providers, improve their security risk profile. SIA and GVF therefore adopt this statement in the interest of promoting development and use of best practices and greater collaboration on important matters of cybersecurity.

SATELLITE INDUSTRY LEADERSHIP IN CYBERSECURITY COLLABORATION

The satellite industry's foundational and long-standing commitment to cybersecurity is evident in recent efforts. Several SIA and GVF member companies participated in the Federal Communications Commission's (FCC's) Security, Reliability, and Interoperability Council IV Working Group 4 (CSRIC IV WG 4) on *Cybersecurity Risk Management and Best Practices*. This substantial effort convened stakeholders from across the communications sector. The satellite segment created a prioritized adaptation of the United States National Institute of Standards and Technology's (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* (*Cybersecurity Framework*), emphasizing the importance of organizations' risk management using flexible measures that are self-reinforcing, tailored to networks' unique needs, and that build upon international standards.

GVF's Cybersecurity Task Force has convened equipment manufacturers and service providers to identify and implement security best practices. As with other cybersecurity efforts, these efforts are designed to help companies develop internal cybersecurity approaches, which should be regularly revisited over time.

Members of both associations continue to participate in various security efforts with government agencies, industry working groups, and international standards bodies. The satellite industry n

Department of Homeland Security, NIST, and others pursuant to executive orders, directives, and initiatives. In particular, programs emphasizing the protection of critical infrastructure and promoting

sharing of threat information reduce overall cybersecurity risk today, and will continue to do so in the future.

International efforts also are a key component of ensuring cyber security for the nation's communications networks. For nearly a decade, the International Telecommunication Union has led cybersecurity initiatives that inform much of today's cybersecurity dialogue, and myriad other national governments and regional groups have taken important steps to promote cybersecurity dialogue and development of best practices. Outside of government-sponsored initiatives, many industry-led efforts have proven effective at developing cybersecurity best practices and sharing valuable information. The industry also strongly supports the work of internationally recognized standards development organizations, the output of which will inform ongoing security specification and process development. The satellite industry's success would not be possible without the foundation laid by these groups.

SIA and GVF members have learned important lessons for effective cybersecurity. Security and risk management must be part of an organization's overall corporate culture. Organizations should, and do, implement best practices to protect against evolving threats and regularly revisit them. Industry members can use the output of CSRIC IV WG 4, the GVF Cybersecurity Task Force, the NIST *Cybersecurity Framework*, and other industry-driven resources to inform their own development of voluntary, proactive, risk-based internal approaches to mitigate risks. Collaboration, not regulation, is the best way for organizations to manage cyber risks. Voluntary information-sharing among the private sector, between the private sector and government, and between the private sector and end users is vital.

CORE PRINCIPLES FOR CYBERSECURITY

SIA and GVF encourage all segments of the satellite industry—from satellite communication providers to equipment manufactures and vendors—to address the dynamic challenge of cybersecurity. SIA and GVF have identified three principles that—although not intended to be a comprehensive roadmap or exhaustive list—should be at the center of private and government efforts to promote national and global cybersecurity.

Voluntary, industry-led efforts and public-private partnerships are the optimal way to address cybersecurity at the national or international levels.

- Cybersecurity solutions are not one-size-fits-all. Networks differ, risk profiles vary, and a potential vulnerability can be addressed in a variety of ways. Thus, to be effective, satellite providers, resellers, software providers and equipment manufacturers must be free to apply security strategies that fit their individual security profiles and preferences.

- Solutions must be flexible and industry-driven, because vulnerabilities and the threat landscape evolve rapidly. Regulatory mandates would become rapidly outdated and would stifle progress by enforcing a static mindset, focused more on regulatory compliance than real-world cyber-risks. Market-driven solutions offer the most flexibility and promote innovation in services and security. While companies must choose what specific processes and practices are right for themselves, standards developed by internationally recognized standards development organizations often represent best practices in security and are excellent choices for many organizations. Likewise, voluntary public-private partnerships have been at the center of

cybersecurity policy, and participation by government and industry should continue to be encouraged.

- There is no such thing as perfect security. Use of cybersecurity standards and practices does not provide immunity from attack. Technical specifications and internationally recognized standards have value and can help improve security, but organizations also should actively monitor threats and revise practices based on changing security environments.

- Organizations' approaches to cybersecurity, and the various policies and procedures they implement, should be regularly reviewed and updated. Today's threats are unlikely to be the threats of tomorrow. Business processes and priorities change. To be effective, best practices and standards—like internal approaches, policies, and procedures—should be "living documents" that not only provide guidance and anticipate present needs, but can be modified to mitigate new risks.

- Trustworthy service offerings depend on trustworthy infrastructure components and practices, as well as reliable partners. This means that security and risk management should be considered throughout the service delivery chain, from network, hardware and software design to manufacturing processes, vendor management, and customer interfaces.

Satellite industry organizations should actively address cybersecurity using industry best practices for risk management.

Each company in the satellite ecosystem should develop its own risk management approach, including by assessing whether to implement or customize one or more of many available tools.

- All organizations should consider adapting information security risk management principles, such as those reflected in the ISO 27001 standard, the NIST *Cybersecurity Framework*, or other relevant guidance documents, for use within their own enterprises. Some companies may use the NIST *Cybersecurity Framework*, as appropriate, to develop their own enterprise-wide approach to securing critical infrastructure, focusing on Identifying, Protecting from, Detecting, Responding to, and Recovering from cyber threats. In this, the illustrative work of CSRIC IV WG 4 may be helpful. A satellite industry member may wish to take approaches to managing security risks not identified here.

- Equipment vendors should consider implementing product security specifications and vendor security processes based on industry best practices and international standards, tailored for the needs of the organization and its customers.

- Service providers should consider security management practices and their technical implementation, which should be adjusted as appropriate for each organization. This approach is intended to be iterative and repeated, allowing companies to learn and adapt their approaches.

- Organizations should consider their processes for identification, intake, and analysis of vulnerability information. Specifically, organizations may benefit from developing and implementing mechanisms for receiving vulnerability information from diverse internal and external sources, evaluating risks, and taking appropriate responses, including through responsible disclosures of this sensitive information.

Robust cybersecurity is aided by voluntary information sharing, free from fear of adverse consequences.

Sector participants often face common threats, so they must be free to collaborate among themselves and with government to identify and respond to attacks, share mitigations, and learn from past experiences.

- Voluntary information sharing can be a critical part of private sector cybersecurity. SIA and GVF support recent efforts to expand and encourage voluntary information sharing. For example, we look forward to the creation and refinement of processes set in motion in the United States by the Cybersecurity Information Sharing Act of 2015 and other federal efforts.

- Information sharing can help identify threats, minimize risk, and keep networks secure. Information should be shared between commercial organizations, commercial organizations and the government, and commercial organizations and the public. Industry members should consider participation in various information sharing mechanisms, including formal and informal groups, and public or confidential processes, as appropriate.

- It is critical that exchanged information be confidential, secure, and used only for purposes of strengthening security and combatting bad actors. Information about threats, mitigations, business processes, or capabilities is competitively sensitive and, in the wrong hands, can aid bad actors. Likewise, companies should not fear that information shared or assistance sought will result in liability, enforcement action, or regulation. The private sector needs assurance that disclosures made to each other, to the government, or that are responsibly made to the public will be used to help protect the organization, the sector, and end users or the public; it should not be used against the organization.