Before the
Federal Communications Commission
Washington, D.C. 20554

In the Matter of	)	
	)	
FCC's Public Safety and Homeland Security	)	PS Docket No. 15-68
Bureau Requests Comment on CSRIC IV	)	
Cybersecurity Risk Management and	)	
Assurance Recommendations	)	

COMMENTS OF THE SATELLITE INDUSTRY ASSOCIATION

The Satellite Industry Association ("SIA")[1] hereby responds to the Federal Communications Commission's ("Commission") Public Safety and Homeland Security Bureau request for comment on the Communications Security Reliability and Interoperability Council IV ("CSRIC IV") Working Group 4 Report on cybersecurity risk management.[2] SIA commends the Commission for enabling and supporting the Working Group's efforts to bring a diverse

[1] SIA is a U.S.-based trade association providing worldwide representation of the leading satellite operators, service providers, manufacturers, launch services providers, and ground equipment suppliers. Since its creation twenty years ago, SIA has advocated for the unified voice of the U.S. satellite industry on policy, regulatory, and legislative issues affecting the satellite business. For more information, visit www.sia.org. SIA Executive Members include: The Boeing Company; The DIRECTV Group; EchoStar Corporation; Intelsat S.A.; Iridium Communications Inc.; Kratos Defense & Security Solutions; LightSquared; Lockheed Martin Corporation; Northrop Grumman Corporation; SES Americom, Inc.; SSL; and ViaSat, Inc. SIA Associate Members include: ABS US Corp.; Airbus DS SatCom Government, Inc.; Artel, LLC; Cisco; Comtech EF Data Corp.; DRS Technologies, Inc.; Eutelsat America Corp.; Glowlink Communications Technology, Inc.; Harris CapRock Communications; Hughes; iDirect Government Technologies; Inmarsat, Inc.; Kymeta Corporation; Marshall Communications Corporation.; MTN Government; O3b Limited; Orbital ATK; Panasonic Avionics Corporation; Row 44, Inc.; TeleCommunication Systems, Inc.; Telesat Canada; TrustComm, Inc.; Ultisat, Inc.; Vencore Inc.; and XTAR, LLC.

[2] FCC's Public Safety and Homeland Security Bureau Requests Comment on CSRIC IV Cybersecurity Risk Management and Assurance Recommendations, PS Docket No. 15-68, *Public Notice*, DA 15-354 (rel. March 16, 2015) ("Public Notice"). *See also* The Communications Security, Reliability and Interoperability Council IV, Working Group 4 Final Report, *Cybersecurity Risk Management and Best Practices* (March 2015) ("Working Group 4 Report").

group of stakeholders together to evaluate cybersecurity risk management approaches. The Working Group 4 Report is a significant contribution to the national discourse on cybersecurity and represents a key step toward achieving Chairman Wheeler's vision of a "new paradigm,"[3] characterized by voluntary processes and assurances rather than regulatory burdens and enforcement mechanisms. SIA supports these voluntary, industry-led efforts to combat cybersecurity challenges and its members look forward to continuing to work—with the Commission as well as through diverse private sector and public-private initiatives—to study and address these issues as they continue to evolve.

I. SIA SUPPORTS THE WORKING GROUP 4 REPORT'S VOLUNTARY APPROACH TO MANAGING CYBERSECURITY THREATS.

SIA applauds the Commission for convening a large and prestigious group of diverse experts to compose the Working Group 4 Report. Working Group 4 consisted of more than 100 cybersecurity professionals from across the communications sector, charged with "develop[ing] voluntary mechanisms to provide macro-level assurance to the FCC and the public that communications providers are taking the necessary corporate and operational measures to manage cybersecurity risks across the enterprise."[4] The group was divided into five industry subgroups, representing the broadcast, cable, satellite, wireless, and wireline segments. Five subject matter-specific "feeder" groups also addressed Cyber Ecosystem and Dependencies, Top Threats and Vectors, Framework Requirements and Barriers, Small and Medium Businesses, and Measurements. To complete their assigned mission, the subgroups met individually, jointly, or

[3] Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute (Jun. 12, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

[4] Federal Communications Commission, *CSRIC IV Working Group Descriptions and Leadership*, *available at* http://transition.fcc.gov/bureaus/pshs/advisory/csric4/CSRIC%20IV%20Working%20Group%20Descriptions%2010%2023%2014.pdf (Oct. 23, 2014).

as the entire working group, often multiple times a week, over the course of a year. The end product is a detailed analysis of the current state of cybersecurity risk management in the communications sector with practical recommendations for how industry, government, and other stakeholders can collaborate to improve cybersecurity and build trust.

Working Group 4 took as its starting point the National Institute for Standards and Technology ("NIST") Cybersecurity Framework ("NIST framework"), a product of industry and government collaboration which "uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses."[5] Preserving this emphasis on critical infrastructure protection and a holistic, enterprise-wide approach to cybersecurity risk management, Working Group 4 undertook to adapt the cross-sectoral NIST Framework to the communications sector. One of the most significant aspects of the Working Group 4 Report is the CSRIC's evolution away from a prescriptive "controls-based" approach to cybersecurity, characterized by the promulgation of hundreds of discrete cybersecurity best practices, toward a risk management approach informed by the NIST Framework.

As applied to cybersecurity, a risk management focus has significant benefits over the best practices approach traditionally used by the CSRIC and its predecessors. A risk management approach is best-suited to keep pace with rapidly evolving cybersecurity threats. The CSRIC has harnessed public and private sector expertise to develop specific best practices on a wide range of communications reliability issues, and it continues to be an effective vehicle for "deep-dive" examinations of complex technical and policy issues outside of the rulemaking context. As the Working Group 4 Report correctly notes, however, "[m]any in government and

[5] National Institute of Standards and Technology, *Framework for improving Critical Infrastructure Cybersecurity* 1 (Feb. 12, 2014) ("NIST Framework").

the private sector have come to understand that the traditional multi-year CSRIC review cycles can no longer keep pace with the accelerating deployment of new network and edge technologies across the ecosystem along with the rapid advancements in increasingly inexpensive, perishable, and more sophisticated cyber threats."[6] By focusing on governance, internal communication, external information exchange, and constant reflection and process improvement, a risk management approach can better address the constantly-changing cyber threat landscape than a prescriptive checklist or rigid best practices approach, which may become outdated before the ink has even dried. Because efforts to help enterprises "manage cybersecurity risk must be continuous and ongoing" to stay ahead of the dynamic cybersecurity curve, collaborative, voluntary solutions are best-suited to meet sector-specific cybersecurity challenges.[7]

The CSRIC's movement toward a voluntary risk management approach to cybersecurity issues aligns with the Commission's current preference for encouraging voluntary, industry-driven solutions to cybersecurity challenges. Indeed, Chairman Wheeler has emphasized the importance of moving toward a "new paradigm for cyber readiness" that primarily relies on "private sector-led effort[s]" and "the market."[8] In line with these principles, the voluntary, risk-based model contemplated by the Working Group 4 Report empowers communications sector members to examine the needs, vulnerabilities, and capabilities of their individual enterprises and develop well-tailored response processes. Importantly, industry-led voluntary approaches such as these permit flexible, innovative solutions to the formidable technical puzzles likely to arise as cybersecurity threats continue to evolve and multiply. To this end, the Working Group 4

[6] Working Group 4 Report at 11.

[7] *Id.* at 10.

[8] Remarks of FCC Chairman Tom Wheeler, American Enterprise Institute, at 1 (Jun. 12, 2014), *available at* https://apps.fcc.gov/edocs_public/attachmatch/DOC-327591A1.pdf.

Report appropriately promotes approaches that can be “[t]ailored by companies to meet their individual needs.”[9] Cybersecurity threats will no doubt continue to develop and evolve over time. The Commission should preserve the flexibility inherent in the Working Group 4 Report’s voluntary approaches it evaluates solutions for managing diverse cybersecurity challenges.

II. THE SATELLITE SUBGROUP REPORT HIGHLIGHTS AND ADVANCES SATELLITE INDUSTRY EFFORTS TO IMPROVE CYBERSECURITY.

As part of Working Group 4’s comprehensive effort, a satellite subgroup focused on “adapting the NIST Cybersecurity Framework, and its emphasis on cybersecurity risk management, to the satellite communications industry.”[10] Composed of diverse stakeholders, the subgroup included service providers and manufacturers in the fixed, mobile, and direct-to-home broadcasting satellite services.[11] As the satellite subgroup noted, satellite communications systems are “key to many critical infrastructure sectors” including emergency services, national defense, and the communications industry.[12] “In each of these sectors, satellite communications provide a primary mechanism for mission critical communications.”[13] Moreover, “satellite communications are unique among communications technology in terms of their ubiquity and survivability, and therefore have additional importance as backup systems for many other sectors.”[14] Whether it is in the wake of disasters that have disabled terrestrial communications,

[9] Working Group 4 Report at 6.

[10] *Id.* at 93.

[11] *See id.* at 93-94.

[12] *Id.* at 93

[13] *Id.*

[14] *Id.*

or to provide reliable, day-to-day communications in harsh, remote environments, satellite systems are an indispensable part of the nation's communications infrastructure.

Satellite industry members have long been leaders in terms of security and reliability. "In particular," as the satellite subgroup report noted, "to support the demands of military and government users, many satellite operators already comply with various controls, checklists, and certifications – including DoD Information Assurance requirements, international standards, and other criteria."[15] Because of the infrastructure components shared between military/government satellite services and those offered to the commercial and enterprise sectors, these protections increase security and reliability for all users of satellite services. The satellite subgroup correctly noted that "[t]his means that satellite communications service providers are leaders in areas like encryption, access control, and overall system hardness."[16] The industry looks forward to continuing to lead in these respects, and has already established several working partnerships with cybersecurity stakeholders within the U.S. government to discuss best practices and address practical issues.

The Working Group 4 satellite subgroup should be commended for its important contributions to analyzing and reporting on cybersecurity risk management frameworks from the perspective of some members of the satellite industry. SIA notes that the satellite subgroup's report diagrams elements of the satellite system, identifies critical infrastructure elements that the subgroup's members determined require protection, and examines the risk management functions, categories, and subcategories set forth in the NIST framework.[17] Further, the satellite

[15] *Id.* at 94.

[16] *Id.*

[17] *See id.* at 93-102.

subgroup produced an illustrative adaptation of the NIST framework for use in the satellite industry, developing use cases and identifying satellite-specific recommendations and informative references.[18] Bringing a wide cross-section of interested stakeholders together to examine the complex technical challenges raised by cybersecurity threats in the satellite industry is a welcome path forward for the Commission's approach to managing cybersecurity risks in the future. SIA supports collaborative efforts such as these that culminate in voluntary, industry-led mechanisms for meeting rapidly evolving cybersecurity threats.

III. CONCLUSION.

SIA appreciates the opportunity to comment on the CSRIC IV Working Group 4 Report. As explained herein, SIA supports voluntary, industry-led approaches to managing dynamic cybersecurity risks across communications enterprises. Satellite industry members will continue collaborating among themselves and with diverse public and private sector partners to improve overall security and enhance the reliability of communications infrastructures.

Respectfully submitted,

/s/ Tom Stroup
Tom Stroup
President
Satellite Industry Association
1200 18th Street, NW Suite 1001
Washington, DC 20036

May 29, 2015

[18] *See id.* at 103-116.