JOINT STATEMENT ON THE SATELLITE INDUSTRY'S COMMITMENT TO CYBERSECURITY AND A SECURE SUPPLY CHAIN

The Satellite Industry Association (SIA), Global VSAT Forum (GVF) and the EMEA Satellite Operators Associations (ESOA). SIA, GVF, and ESOA on behalf of their members, issue this joint statement on the industry's commitment to cybersecurity.

Cybersecurity and a secure supply chain 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.

Communications has become a key enabler for nations to enjoy vibrant 21st Century economies and an equally important contributor to governments maintaining sovereignty and security, resulting in increasing numbers and continuously evolving attacks by criminals, terrorists and nation-states, engendering mounting concern by leaders in the private and governmental sectors. 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, GVF, and ESOA 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 and a secure supply chain is evident in recent efforts. Several SIA, GVF and ESOA member companies have participated in governmental efforts that convened stakeholders from across the communications sector. The satellite segment created guidance, 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 notes the work completed through programs emphasizing the protection of critical infrastructure and promoting the sharing of threat information serves to 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 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, GVF, and ESOA members have learned important lessons for effective cybersecurity and a secure supply chain. 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 ISO 27001 Document Bodies 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, GVF, and ESOA encourage all segments of the satellite industry—from satellite communication providers to equipment manufactures and vendors—to address the dynamic challenge of cybersecurity. SIA, GVF, and ESOA 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 and a secure supply chain 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 and supply chain. 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 supply chain security, 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 and supply chain security 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, or other relevant guidance documents, for use within their own enterprises. Some companies may use such guidance, 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. 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 and supply chain security 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 and supply chain security. SIA, GVF, and ESOA support recent efforts to expand and encourage voluntary information sharing.

- 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.