WHITE PAPER

INTELSAT

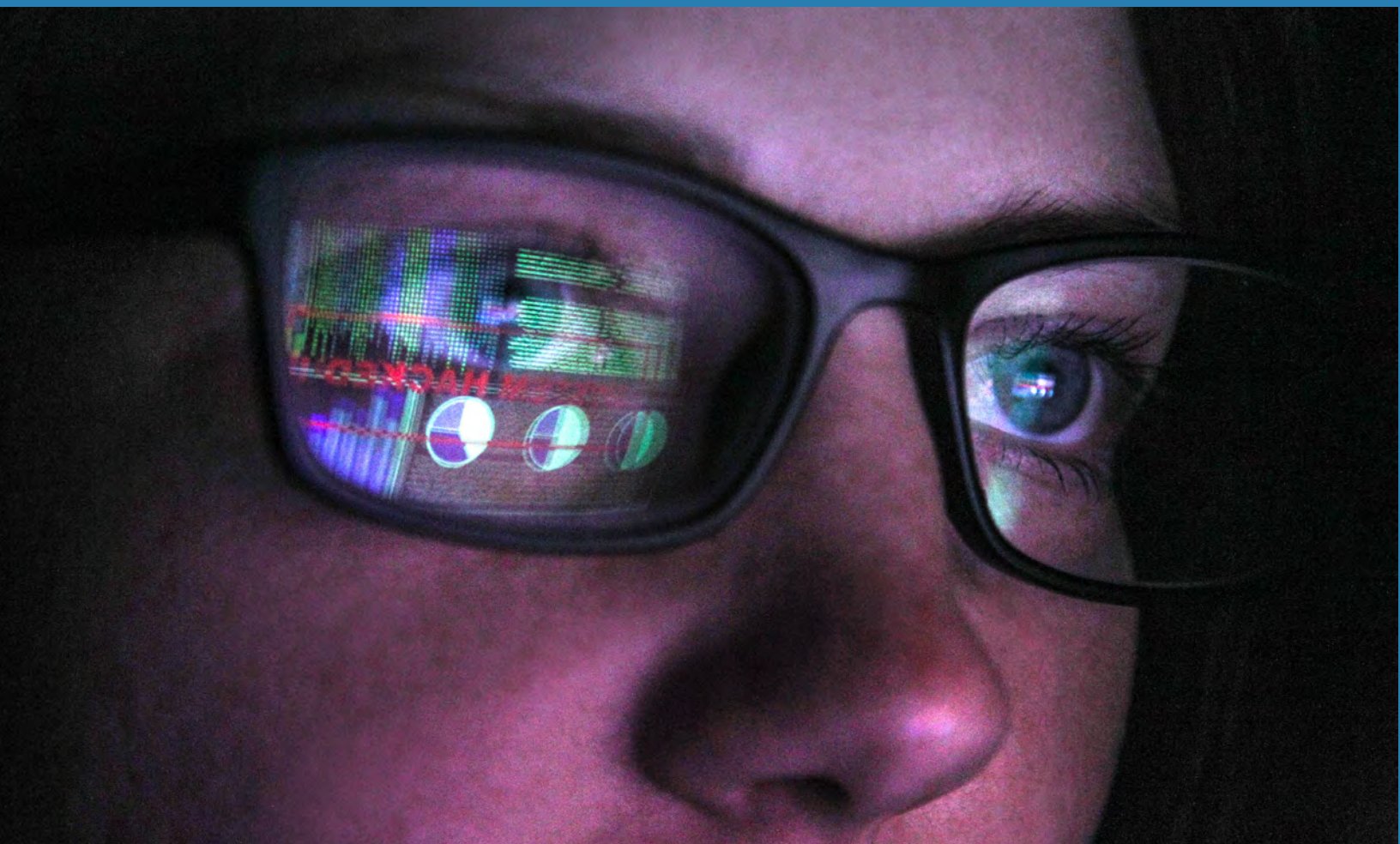
Security in Space: Intelsat Cybersecurity

Summary

Securing satellite networks is a complex undertaking given the nature and scope of the satellite ecosystem. Given the expansion of 4G/5G networks, it is no longer enough to focus on securing the satellite itself as the typical satellite network architecture is global, spans both terrestrial and satellite links as well as cellular, internet and/or microwave connections.

As a result, the challenge is to ensure that the entire ecosystem, not just your company, has the right security posture to harden your company against the gamut of attacks pervasive in today's environment. The threats, might originate from both internal and external sources. They can be in the form of Spam, Spear Phishing, Distributed Denial of Service, Interference, Targeted Malware, Data Loss & Interception and State Sponsored. It is no longer enough to make sure that your satellite infrastructure has the right security policies and procedures in place, but that your equipment providers and customers have implemented layered controls and countermeasures to help mitigate the risk of an attack that could impact the entire ecosystem.

For more information, we invite you to talk to our experts and discuss your specific requirements. Contact us by visiting **www.intelsat.com.**



Intelsat Information Assurance

Intelsat maintains the highest standards of Information Assurance by assessing and building the Intelsat infrastructure, networks and third party infrastructures against applicable National Institute of Standards and Technology (NIST) Risk Management Framework (RMF) security controls. Intelsat's Information Assurance program focuses on prevention and restoration by taking a systematic defense-in-depth approach that detects, prevents and mitigates attacks enhancing resilience and mission assurance in its satellite, ground and network infrastructure.

The program is centrally managed by Intelsat's Information Security team which is the authority for all Intelsat Information Assurance policies. Further, Intelsat maintains a comprehensive Information Assurance assessment and remediation program that includes annual penetration assessments, organization-wide control assessments and independent third-party Service Organization Control 3 (SOC3), Cybersecurity Maturity Model Certification (CMMC), and Infrastructure Asset Pre-Assessment (IA-Pre) assessments. The audits against Intelsat's satellite and terrestrial service environments include Intelsat's satellite commanding, teleport, terrestrial and service management infrastructure and relevant service procedures.

Information Assurance Program

Intelsat's Information Security function centralizes global responsibility for Information Assurance while basing its control framework on ISO 27001, RMF, CMMC, and IA-Pre. Information Security works proactively to maintain the availability, integrity and confidentiality of Intelsat data and applications throughout its service and enterprise networks.

Information Security Framework

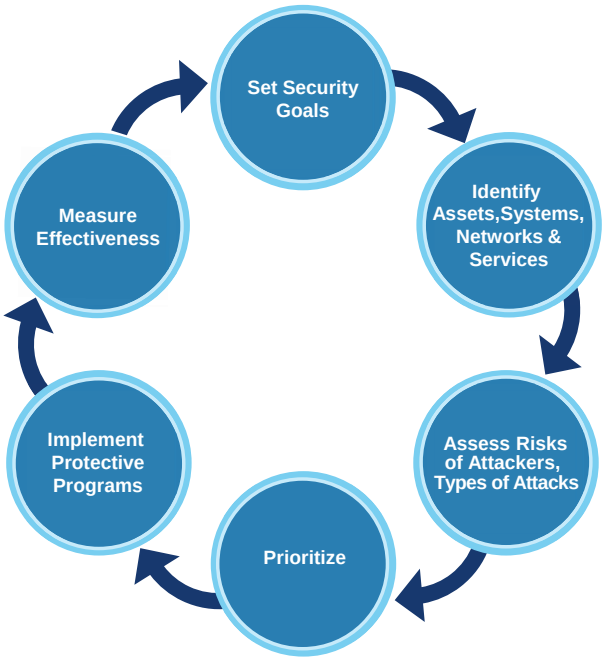
Intelsat's Information Security framework addresses continuously evolving threats and risks using a lifecycle approach that consists of the following phases:

- Set security goals
- Identify assets, applications, networks and services
- Assess risks (consequences vs probability of vulnerabilities and threats)
- Prioritize
- Implement protective programs
- Measure effectiveness
- Continuously monitor

Information Security implements its framework to address the following across its service and enterprise networks:

- Information Security compliance
- Policy
- Access control
- Risk management
- Remote access
- Awareness and education
- Network management applications
- Secure design and configuration
- Security information and event management

Figure 1: Information Security Framework



Information Security Compliance

Intelsat developed its Information Security framework utilizing the security controls from multiple industry standards and government regulations. Intelsat adheres to and assesses against the following:

- ISO 27001/

Information Security Countermeasures

Intelsat employs relevant and layered counter-measures to combat the most advanced threats against industry and government. Intelsat continuously evaluates the threat landscape and the effectiveness of its countermeasures; adjusting and adapting to the latest threat actors and attack methods.

Figure 2: Security Countermeasures are categorized as:

Preventative	Detective	Access & Authentication	Management
			
▪ Advanced Threat Management ▪ Intrusion Prevention Systems ▪ Application Control ▪ Inline Web and Email Analysis ▪ Command Encryption	▪ Network Threat Detection ▪ Host Threat Detection ▪ Distributed Denial of Service Management ▪ Active Cooperative Intelligence	▪ Identity Management ▪ Multi-Factor Authentication ▪ Virtual Private Networks Network Segmentation ▪ Active Password Management ▪ Secure Commanding	▪ Security Event Management ▪ Central Access Management ▪ Central Endpoint Management ▪ Advanced Configuration Management

Intelsat's Service Infrastructure is Designed for Reliability

Intelsat's fleet of satellites provides communications services to 99 percent of the world's populated regions. Intelsat's fleet is resilient; in many cases satellite capacity is available to restore services in the event of a major outage on the customer's primary satellite. For satellite monitoring and control operations, Intelsat operates fully redundant operations centers in McLean, VA and Long Beach, CA with a redundant and tertiary global architecture.

Access to Intelsat's global fleet is provided by a collection of teleports designed to support customer applications ranging from broadband services to television programming distribution. Backup for satellite uplinks and downlinks at Intelsat's teleports allows Intelsat to minimize down time in case of outages, or when inclement weather affects the quality of the signal at the customer's primary teleport facility.

IntelsatOne® is a global, terrestrial architecture, consisting of an Internet Protocol (IP) / Multiprotocol Label Switching (MPLS), fiber, teleport, and points of presence (PoP) service network.

The architecture is integrated and complements Intelsat's global satellite fleet, providing a single source for converged voice, video, and data solutions. The IntelsatOne design includes alternative fiber routing with redundancy built into the connectivity to its teleports, major media hubs and city PoPs to back up customers' primary fiber paths.

IntelsatOne provides a converged carrier-class network that integrates and extends multi-services, such as media and data services, for a variety of customer applications. The network integrates terrestrial and satellite access technologies to facilitate end-to-end service delivery models.

The IntelsatOne network is further supported by management and administration applications that are used to provide control and oversight of the Intelsat service infrastructure. Ground applications are used for purposes of controlling teleport equipment and equipment utilized for uplink and downlink capabilities.

Intelsat's Service Procedures are Fully Integrated with Our Information Assurance Program

Satellite Commanding

Intelsat follows established procedures for commanding Intelsat and third-party satellites. Command procedures are documented, controlled and managed, and are independently verified. Pre-approved commands are selected from a command database and require verification prior to transmission. For command security, Intelsat employs a tactical combination of facility, RF and command encryption practices to provide a layered structure for secure commanding.

Meetings are held each weekday to review operational activities for the prior period and discuss the upcoming period. Each Satellite Operation Center serves as a fully redundant hot standby for the other center. Each Satellite Operation Center can command the entire fleet at any time and can transmit commands utilizing multiple teleports. In addition, each center can remotely operate the other center's equipment, which minimizes the time for transfer. The Intelsat General Security Operations Center (ISOC) is manned around the clock to monitor satellite function and security for IGC's customers.

High Availability

High availability and resiliency are incorporated in the design, implementation and operations of Intelsat's network services. Intelsat follows standard procedures to help ensure assets are operating in a normal state and takes appropriate action to investigate and remediate events. In addition, regular preventative and corrective maintenance is performed to identify equipment in need of maintenance or replacement prior to an actual failure.

Change Management

Intelsat utilizes change management procedures to minimize the potential for disruption to services while emphasizing logging and auditing for correlation and event notification. Change requests are communicated to multiple departments as part of change management procedures and reviewed prior to scheduling and implementation. Critical operations and associated technologies follow a business continuity and disaster recovery process along with testing to help ensure the operability of disaster recovery sites.

Physical and Logical Access Control

Intelsat also employs layers of physical security controls and processes at its locations, including gated access, security cameras, badge controlled access and manned security desks at primary entry points. Additional physical controls are implemented within critical operations areas and Satellite Operations reside in a segmented protected environment. Procedures related to logical access control are centrally managed within their respective environments and are based on the principles of authorized approval, least privilege, role-based access and segregation of duties. All network segmentation and network access controls are managed and overseen by Intelsat Information Security.

Further Detail on Intelsat's Leading Information Assurance Program

Intelsat regularly meets with its customers to discuss information assurance concerns and areas for collaboration to improve the mutual environment. If your company is interested in further discussing Information Assurance and your network environment, please contact your sales representative to schedule a session.

About Intelsat

As the foundational architects of satellite technology, Intelsat operates the largest, most advanced satellite fleet and connectivity infrastructure in the world. We apply our unparalleled expertise and global scale to reliably and seamlessly connect people, devices and networks in even the most challenging and remote locations. Transformation happens when businesses, governments and communities build a ubiquitous connected future through Intelsat's next-generation global network and simplified managed services.

At Intelsat, we turn possibilities into reality. Imagine Here, with us, at Intelsat.com.

Contact Sales

Africa
+27 11-535-4700
sales.africa@intelsat.com

Asia-Pacific
+65 6572-5450
sales.asiapacific@intelsat.com

Europe
+44 20-3036-6700
sales.europe@intelsat.com

Latin America & Caribbean
+1 305-445-5536
sales.lac@intelsat.com

Middle East & North Africa
+971 4-390-1515
sales.mena@intelsat.com

North America
+1 703-559-6800
sales.na@intelsat.com

Intelsat General
+1 703-270-4200
sales.inquiries@intelsatgeneral.com

www.intelsat.com

INTELSAT

20/10/6997 Security in Space