WHITE PAPER

INTELSAT

Security in Space:
Intelsat Cybersecurity

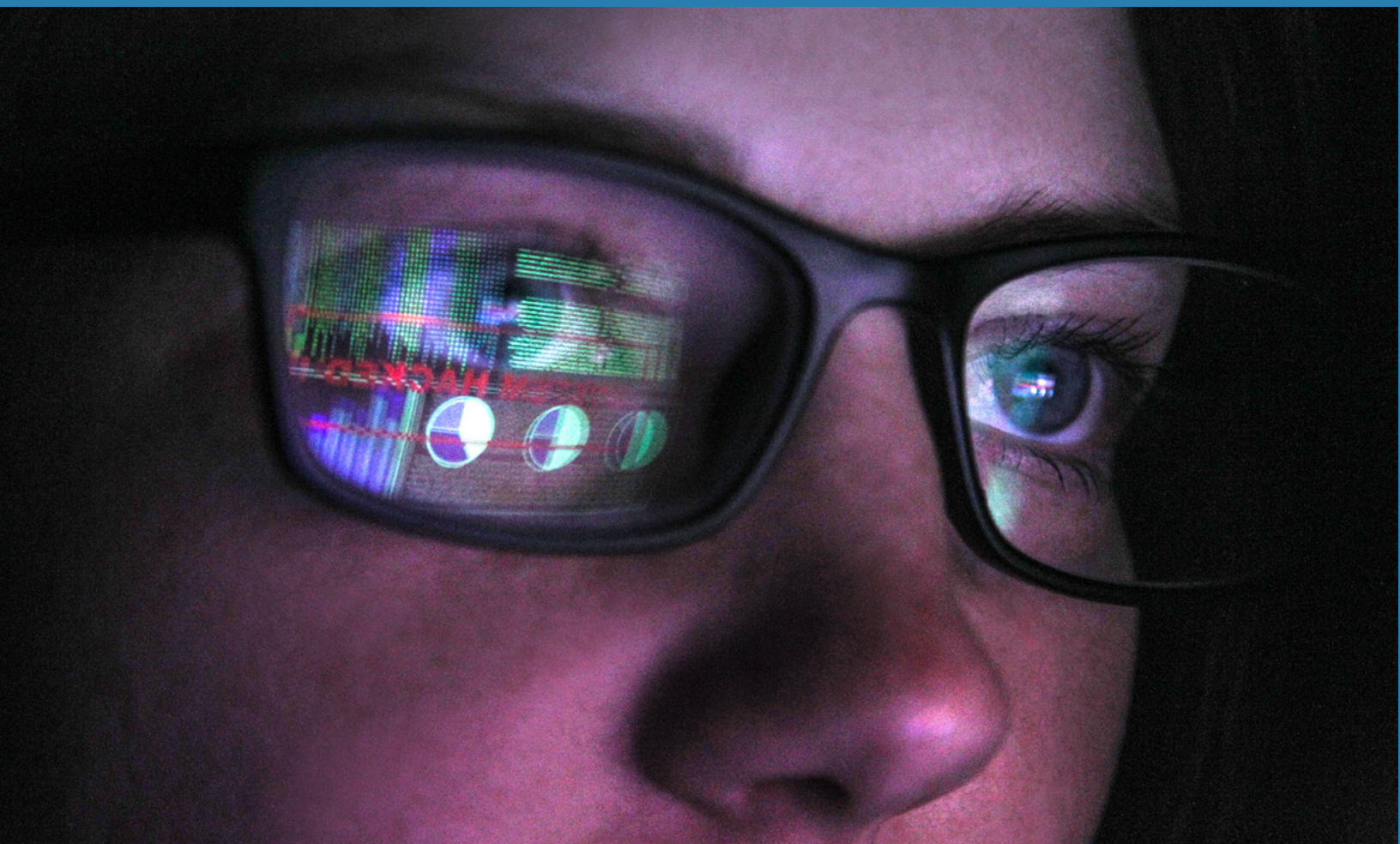
Introduction

With the development of global networks, focusing on protecting the satellite itself is no longer enough. Intelsat's priority is to ensure that the entire ecosystem has the right system security so it can be protected against the wide spectrum of today's attacks.

Information security as a practice continues to evolve; where once the focus was technical controls and clear boundaries, we now face increasing compliance requirements through laws, regulation, customer expectations as well as the erosion of the traditional corporate network edge.

Given the expansion of terrestrial networks like 4G/5G, 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 Intelsat, has the right security posture to harden its costumers 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 and 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 threat of an attack that could impact the entire ecosystem.



Intelsat Information Security Program

Intelsat's Information Security program focuses on prevention and restoration enhancing resilience, and mission assurance in its satellite, ground, and network infrastructure.

Intelsat maintains the highest standards for the Information Security Program by assessing and building the Intelsat satellites, infrastructure, networks, and third-party infrastructures against multiple framework, utilizing NIST SP 800-53 rev. 4 as identified within the NIST SP 800-171 rev. 2 as a base.

The 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 Security policies. Further, Intelsat maintains a comprehensive Information Security assessment and remediation program, which includes:

- Recurring penetration assessments
- Organization-wide control assessments
- Third-party Service Organization Control (SOC3) audits against Intelsat's satellite and terrestrial service environments including Intelsat's satellite commanding, teleport, terrestrial, and service management infrastructure and relevant service procedures.

Components of information security, such as authentication, access rights, and network security are covered in Intelsat's annual Sarbanes-Oxley compliance testing. Further, Intelsat commissions third parties to conduct at least bi-annual penetration testing and comprehensive information security assessments, with action taken to address and mitigate identified vulnerabilities.

Information Security Team

The Intelsat Information Security team is responsible for the identification of current risks associated with Information and Information systems. The team holistically reviews Information Security within Intelsat to ensure confidentiality, integrity, and availability throughout the Intelsat environment, while complying with the strictest international security standards. They use relevant and layered counter-measures to tackle advanced threats against government and industry. The team also collaborates with other IT teams to ensure the safety of both customer information and internal employees.

Information Security Compliance

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

- DOD CMMC
- HIPAA HITECH
- ISO 27001/27002
- NIST SP800-53
- NIST 800-171 rev. 2
- PCI DSS 3.2
- Sarbanes-Oxley
- USSF CSCO IA-Pre

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, vulnerabilities, and threats)
- Prioritize
- Implement protective programs
- Measure the effectiveness

Figure 1: Information Security Framework

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

Security is Our Top Priority

Network and System Security

The Information Security team ensures that the Intelsat network, its intellectual property, the privacy of staff and customer information are secure, by identifying existing vulnerabilities and ensuring the remediation of those vulnerabilities, and by investigating information security attacks that arise. Intelsat has implemented a SIEM system that consolidates audit records from firewalls, IDS/IPS, servers, cloud service providers, databases, web applications, physical security systems and other equipment as appropriate. The system acts as an automated and continuous monitoring utility capable of auditing and reporting.

Intelsat implements layered security controls which include multiple layers of Network Based firewalls, VPN, Intrusion Detection and Prevention Systems, advanced content analysis and filtering, vulnerability management, and end-point protection. These end-point protections include anti-virus, host-based IDS/IPS, application controls, and advanced hardening procedures that reside on satellite control systems.

Security at Home

Every day, malicious content is found across the internet, such as viruses, worms, trojans, and email scams. While the number of people working from home keeps rising, Intelsat takes the security of the company's information data very seriously.

Security of the operating system and vulnerable applications is of the utmost importance to Intelsat. We ensure the latest software releases and security patches are implemented for all operating systems and applications installed. Also, the Information Security team shares security awareness techniques, as well as training on recognition of potential security threats, to all the information system users.

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 the disaster recovery site.

Physical and Logical Access Control at Intelsat's Facilities

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 resides 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.

Intelsat's Service Infrastructure is Fully Integrated with Our Information Security Program

Intelsat's global network consists of the world's largest satellite fleet working in concert with terrestrial networking infrastructure and robust managed services. Intelsat's capacity is monitored on a 24/7 basis for increased security from interference or unauthorized carrier identification. Our network is highly redundant (resilient) with backup satellite, teleport and fiber path options.

Intelsat's fleet covers 99% of the earth's populated regions, with over 36,000+ miles of terrestrial fiber optic cable and strategically located teleports and Points of Presence worldwide for truly redundant coverage.

Satellite Fleet

Intelsat offers global coverage using multiple frequency bands, and Intelsat Epic satellite technology that delivers high-performance connectivity. Intelsat follows standard procedures to help ensure assets are operating in a normal state, and takes appropriate action to investigate and remediate events. We also maintain EMI/RFI identification, characterization, and geo-location capabilities to support the resolution of purposeful and accidental incidents of interference.

The robust interference geo-location system identifies the geographic source of signals interfering with carriers operating in the system, including the ability to identify and characterize sub-carrier EMI/RFI being transmitted underneath an authorized carrier, and the ability to geo-locate the source of any and all EMI/RFI.

Once transmitters identified through the database search are eliminated as possible sources of interference, we use our worldwide network of geo-location systems to investigate EMI/RFI events at C-, Ku-, Ka- and X- Bands.

Intelsat provides backup solutions for satellite capacity 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.

Intelsat Epic Platform

High-data rates using small mobility antennas are today uniquely possible with Intelsat Epic, the first global Ku-band high-throughput satellite (HTS) platform. This platform is an innovative approach to satellite and network architecture utilizing C-, Ku-, and Ka-bands, wide beams, spot beams, and frequency reuse technology to deliver more throughput per unit of spectrum. Designed as a complementary overlay, Intelsat Epic is fully integrated with Intelsat's existing satellite fleet and our global IntelsatOne terrestrial network.

Advanced digital payload provides enhanced protection against jamming, interference, and other forms of information warfare through spot-beam technology, wider bandwidth beams, and frequency notching.

Terrestrial Network

Access to Intelsat's global fleet is provided by a collection of teleports and fiber network designed to support customer applications ranging from broadband services to television programming distribution.

IntelsatOne is a global terrestrial IP/MPLS-based 10G/100G capable network of 50000+ miles of leased fiber, award-winning teleports, and numerous Points-of-Presence, fully integrated with one of the world's largest satellite fleets. The network offers one simple interface for secure, multiple high-bandwidth applications for a variety of managed, converged services and solutions.

IntelsatOne Terrestrial Fiber Platform is a fully redundant network which includes:

- Enhanced security, with Internet route-free core, traffic separation via MPLS-based VPN capabilities, and security embedded at the service layer.
- Enhanced network products such as IPv6 next-generation IP services, DVB-S2 trunking, and MPLS VPN.
- Increased visibility and control of services operating across the Intelsat network
- Access through at least three different paths to most of IntelsatOne PoPs, allowing you to redirect services across the network during a planned (or unplanned) outage.
- Zero over-subscription to provide enhanced security and allows guaranteed bandwidth for critical services.

Intelsat operates eight teleports located strategically across the globe with:

- Around-the-clock operation centers support and integrated connectivity with Intelsat Cloud partners.
- Backup for satellite uplinks and downlinks which allow Intelsat to minimize downtime in case of outages, or when inclement weather affects the quality of the signal at the customer's primary teleport facility.
- Physical and logical access controls, emergency response teams, redundant infrastructure, diverse operating capabilities and post disaster recovery plans for continuity and security of service

Further Detail on Intelsat's Leading Information Security Program

Intelsat regularly meets with its customers to discuss information security concerns and areas for collaboration to improve the mutual environment. If your company is interested in further discussing our Information Security Program, 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

21/3/6997 Security in Space