Agenda

» Opening Remarks
» Framework
  » Confidentiality
  » Integrity
  » Availability
» Definition, Best Practices, and Real World Implementation
Global Concerns Drive US Government Demand

Complex event-driven global reality
On-demand mobility
Worldwide readiness for the unexpected
High reliability, high throughput
Inmarsat well-matched


Source: Council on Foreign Relations 5 Oct 2015
Markets We Serve

- **Defense** – Our first-hand military experience gives us a unique understanding of net-centric communications for CONUS and OCONUS deployments

- **Federal Civilian** – We understand the government’s need to do more with less, and our solutions allow federal civilian agencies to stay connected while leveraging their existing infrastructure

- **Homeland Security** – Our communication solutions ensure interoperability and rapid response for the organizations dedicated to protecting U.S. assets

- **Public Safety** – We deliver secure, interoperable communication solutions that allow first responders to share information in real time
Availability

Definition

- Information is accessible at all times
- No disruption in services
- No loss or destroyed data
- Information is neither denied nor delayed
Availability

Best Practices

- **Redundancy** – Line of Sight (LOS) and Beyond Line of Sight (BLOS) payloads
- **Resiliency** – Make use of both MILSATCOM and COMSATCOM
- **Segmentation** – segment inbound and outbound, C2 and reachback paths in a range of widely available frequency bands
- **Diversity**
  - develop advanced, disaggregated payloads in diverse spacecraft and orbit slots
  - build flexible “active” payloads with shaping, steering, zooming, spots
Availability

Real World Implementation

Inmarsat L and Ka-band

Resiliency – Make use of both MILSATCOM and COMSATCOM
Availability

Implementation

Diversity – build flexible “active” payloads with shaping, steering, mobility

Redundancy – Leverage both Line of Sight (LOS) and Beyond Line of Sight (BLOS) payloads

GX delivering military-Ka to users across Indian Ocean Region

Dozens of military-Ka terminals type-approved

Global ‘SATCOM as a service’ provides easily used and robust complement to fixed-beam MILSATCOM
Confidentiality

Definition

- Prevent communications from reaching the wrong people
- Ensure that the right people can get to the information
- Access must be restricted to authorized users only
Confidentiality

Best Practices

▷ **Adaptive response** – leverage low probability of intercept, detection, and exploitation techniques

▷ **Deception** – mask or obfuscate frequency band intent and usage for C2 and reachback

▷ **Unpredictability** – random configuration of components and services

▷ **Coordinated defense**
  
  ▶ employ smart antennas, directional, low side-lobe, nulling, narrow spot beams
  
  ▶ use spread spectrum, frequency hopping, scrambled coding, etc.
Deception – mask or obfuscate frequency band or sensor intent and usage for C2 and reachback
Confidentiality
Real World Implementation

Command Origination

Customer - Remote
Customer - Centralized
Service Provider

Delivery Mechanism
- Out-of-band network
- Terrestrial
- L-Band/UHF
- Other DoD System

Implementation

CONUS-based Hosted Ops Center encrypts command

1

Inmarsat SCC inserts encrypted command into T&C stream

2

Inmarsat Teleport Uplinks T&C stream to satellite

3

Secure, autonomous steering control
Confidentiality
Real World Implementation

Discreet SIM
Disable GPS-based location reporting

The Challenge
› User Terminal (UT) contains built-in GPS receiver
› GPS position reported (encrypted) to network as part of registration process
› Special circumstances mean that important government customers may find this facility an obstacle to purchasing the service

Considerations
› Minimum level of UT position reporting for network access is required – spot beam ID
› GPS receiver required in UT in order to determine its location and provide optimised operation

Solution
› Disable through a SIM feature
› UT translates GPS position to a spot beam ID using internal map
› Only spot beam ID reported to network

UT operates discreetly within a spot beam (200 - 600 km diameter)
Authenticity – the ability to verify the content has not changed in an unauthorized manner

Accountability – the origin of any action on the system can be verified and associated with a user

Consistent, accurate, and trustworthy data

Must not be changed in transit
Personnel security – logging/audit trails to see exactly when the system has been entered, whether any data has been changed, and by whom

Physical security of COMSEC equipment IAW FIPS Publication 140-2 (Levels 1 to 4) and TRANSEC

Coordinated defense – randomly reconfigure components and services through segmentation

Dynamic representation – pre-define transmission plans, implemented dynamically, to support continuity and contingency plans
Integrity
Real World Implementation

- Fully redundant regional Satellite Access Stations (SAS) strategically positioned in NATO or Five Eyes countries
- Complement WGS
- Supports govt specified waveforms

- Robust network baselined as US MAC III and up to MAC I via Secure Global Xpress
- Secure gateways and satellite commanding
Integrity
Real World Implementation

The Inmarsat Government Network

Customer Core
Satellite / Teleport
Customer Edge

End-to-End Managed Services

- Secure Gateway Red/Black
- Private Network
- Customer Point of Presence (PoP)
- Area Processing Center
- Secure Gateway Red/Black
- Private Network
- Customer Point of Presence (PoP)
- Area Processing Center

- End-to-End Managed Services
  - Engineering Services
  - Network Operations Security Center (NOSC)
  - Technical Assistance Center (TAC)
  - Global Management System
  - Program / Project Management