ICT PORTAL

The SES Space & Defense ICT Portal is a customizable, consolidated platform for ecosystem management and operations, giving customers near-real-time insight into network performance. Features include trouble ticket tracking, network status down to the end-user device, performance metrics, and project or upgrade updates. Fully compliant with NIST and DoD Risk Management Framework (RMF) standards, the Portal reflects the holistic, technology-agnostic design of the SES Space & Defense ICT Ecosystem. It provides a single, flexible interface for monitoring, managing, and troubleshooting the network end-to-end—empowering customers to visualize their network status directly. By delivering critical information instantly, the ICT Portal enables faster, more informed decisions in high-tempo operational environments. More than an information source, it's a mission-assurance tool that combines comprehensive visibility with operational agility.

The SES Space & Defense ICT Portal provides views into:

SPACE SEGMENT

- Capacity Management
- Spectrum Monitoring
- Bandwidth Forecasting/Reservation*
- AI/ML Capabilities*

GROUND SEGMENT

- End-to-end Configuration Details
- End-to-end Performance Monitoring
- End-to-end Events/Conditions
- Congestion Management*

** future capabilities*

NETWORK MANAGEMENT

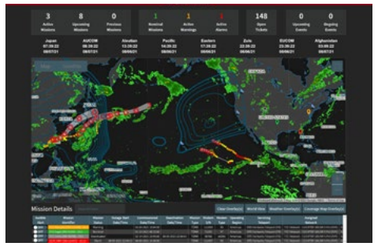
Cybersecurity

- FedRAMP Authorized Cloud Services
- Role Based Access Control

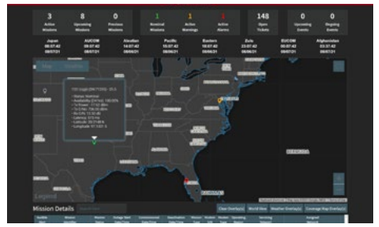
ITSM

- Ticketing/Reporting
- Asset Management
- Knowledge-base
- Ordering/Billing*

Operational Tools



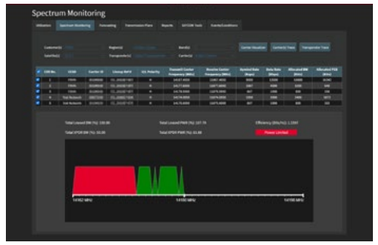
Use satellite footprint and weather overlays to increase situational awareness of network performance



Quickly see critical remote (mission) configuration and performance details at a glance

Focus in on remote (mission) KPIs in the mission performance view

See near real-time satellite transponder spectrum views with Transponder Trace



View carrier and transponder layouts and key metrics with Carrier Visualizer

Easily ensure traffic optimization by determining remote (misson) network traffic consumed by protocol type

ses Space & Defense

ICT PORTAL

A web-based NetOps capability providing a transparent and consolidated view of your network to improve performance and operational decision making.

Visit us at sessd.com

ICT PORTAL

SINGLE PANE OF GLASS NETWORK VISIBILITY

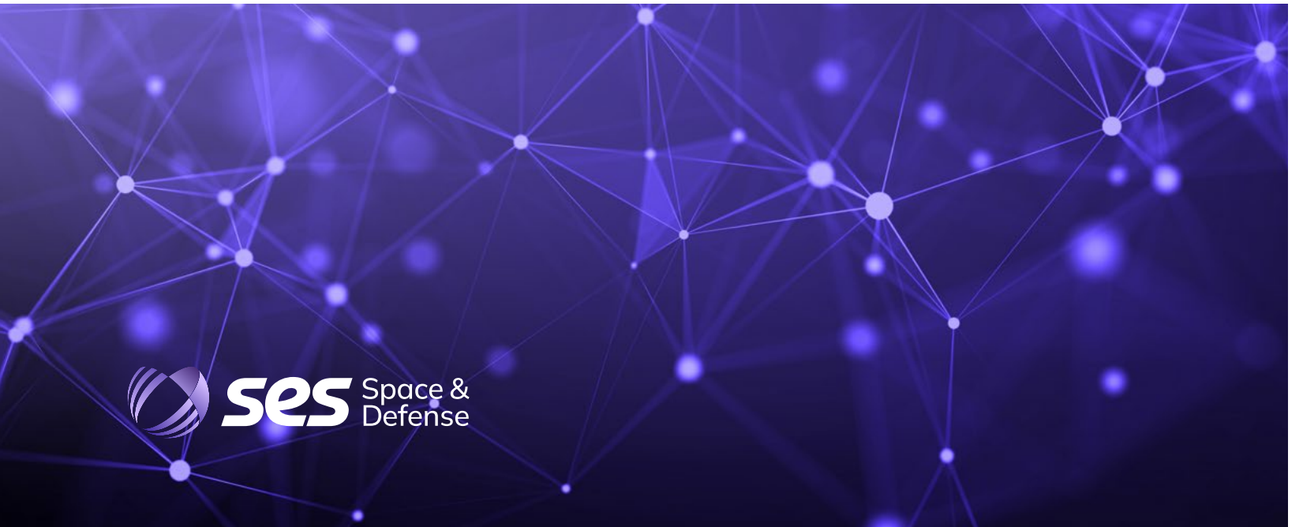
A web-based NetOps capability providing a transparent and consolidated view of your network to improve performance and operational decision making.

The Information & Communications Technology (ICT) Portal from SES Space & Defense is a web-based NetOps capability that can be accessed anywhere in the world and provide a consolidated and transparent view of key information into a customer's network performance, utilization and general situational awareness.

The ICT Portal places precise performance analytics and actionable data in the hands of key decision-makers through near real-time monitoring and reporting capabilities. Users can monitor, from anywhere in the world, hybrid, complex networks consisting of disparate systems, siloed software, multiple nodes, and various types of equipment that inherently do not communicate with one another.

Capability Overview:

- Technology agnostic
- Common operating picture (single pane of glass)
- Modular design - easily customize views and reporting
- Simple and secure login via any IP connection (private network, or firewalled Internet)
- Complete monitoring of network operations for near real-time performance visibility of hybrid terrestrial and satellite wide area networks
- Alarm awareness, predictive troubleshooting via targeted data presentation
- Centralized data repository (resource library)
- Enhanced Information Technology Service Management (ITSM) features and functionality



The ICT PORTAL's Three Pillars of Security

Confidentiality
Ensuring that only authorized persons have access to your information and denying access to those who are unauthorized.

Integrity
Ensuring information cannot be changed undetected by protecting against improper modification and/or destruction with encryption and hashing.

Availability
Ensuring information is available whenever needed, including timely and reliable access, regardless of time of day, location, or other factors.

Protecting the confidentiality, integrity, and availability of public and private sector data is at the forefront of our ICT Portal capability development initiative. Given the increasing need to adhere to FISMA regulatory compliance, SES Space & Defense selected ServiceNow and AWS as key components of the core ICT Portal architecture that drives the front-end portal interface and establishes the back-end data connections. Both vendors maintain FedRAMP High for their Government Cloud services.

Seamless integration with the SES Space & Defense Global Communications Network (GCN) supports current Risk Management Framework (RMF) posture and Authority to Operate (ATO)

The back-end data connections are integrated into the SES Space & Defense Global Communications Network (GCN) which has a U.S. Department of Defense (DoD) Risk Management Framework (RMF) Authorization to Operate (ATO). The SES Space & Defense ICT Portal implements over 180 additional security controls and has a highly trained and dedicated staff of cybersecurity experts to continuously monitor and support the ICT Portal.

Security regulations that SES Space & Defense follows:

- DISA Security Technical Implementation Guides
- Application Development and Security Version 5
- Microsoft SQL Server 2016
- NIST Frameworks
- Risk Management Framework (SP-800-37)
- Security and Privacy Controls for Information Systems (SP-800-53)
- Protecting Controlled Unclassified Information in Non-federal Systems (SP-800-171)
- Continuous Monitoring (SP-800-137)
- FIPS 140-2 (Data at Rest and Data in Transit Encryption)

Security regulations that AWS Gov Cloud and ServiceNow Government Community Cloud follow:

- FedRAMP High Authorization.

Additional ICT Portal security control categories

- Access Control
- Risk Assessment
- Identification and Authentication
- Incident Response
- System and Communications Protection
- Maintenance
- System and Information Integrity
- Media Protection
- Defense in Depth and Boundary Protection
- Contingency Planning
- Physical and Environmental Protection
- Awareness and Training
- Audit and Accountability
- Assessment, Authorization, and Monitoring
- Personnel Security
- Configuration Management
- Vulnerability and Patch Management