

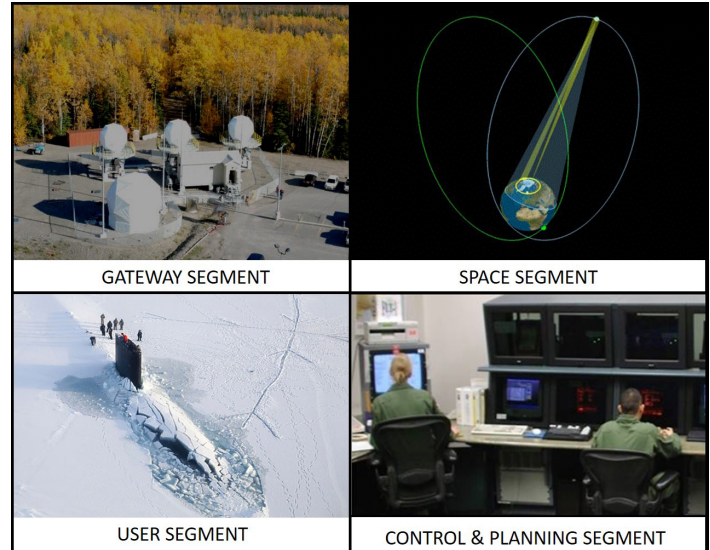
## Enhanced Polar System (EPS)

### Executive Summary

- The Air Force Operational Test and Evaluation Center (AFOTEC), with participation from the Navy Commander, Operational Test and Evaluation Force (OPTEVFOR) conducted a dedicated Multi-Service Operational Test and Evaluation (MOT&E) of Enhanced Polar System (EPS) from March 25 through June 11, 2019.
- The EPS is operationally effective in providing Advanced Extremely High Frequency (AEHF) extended data rate (XDR) satellite communications (SATCOM) to support submarine and surface ship operations in the North Polar Region in benign and threat environments.
- The EPS is operationally suitable. The EPS met the user-defined operational availability and reliability requirement.
- The EPS performs better than the user-defined anti-jam requirement.
- The EPS is secure from cyber-attacks from an outsider threat.

### System

- EPS is designed to provide secure, jam-resistant satellite communications in the North Polar Region using a subset of the AEHF XDR waveform.
- EPS consists of four segments:
  - The Payload Segment consists of two payloads hosted on satellites placed in highly elliptical orbits. The EPS payloads will provide polar communications coverage for 24-hours per day.
  - The Control and Planning Segment (CAPS) is the primary means for monitoring and controlling the payloads via a ground connection to a Tracking and Commanding terminal in the polar region. The Tracking and Commanding terminal will provide radio frequency connectivity between the payload and CAPS.
  - The Gateway Segment consists of a single gateway site with three collocated gateway terminals that will provide radio frequency connectivity between the payload and the gateway ground equipment. The Gateway Segment is also designed to provide ground connectivity between north polar and mid-latitude users through the DOD Teleport System.



- The EPS Terminal Segment consists of user terminals that are Multiband Terminal platform variants. The Navy Multiband Terminals can be deployed on ships and submarines, as well as at specific fixed ground locations. Additional terminals are currently unfunded but may be developed in the future and deployed on aircraft and ground-transportable, mobile, and fixed-terrestrial platforms.

### Mission

Combatant Commanders will use EPS to provide secure, jam resistant tactical satellite communications required to support peacetime, contingency, and wartime operations at high north latitudes with command and control centers located elsewhere.

### Major Contractors

- Northrop Grumman Aerospace Systems – Redondo Beach, California
- Northrop Grumman Mission Systems – Redondo Beach, California

### Activity

- AFOTEC, with OPTEVFOR participation, conducted a dedicated MOT&E from March 25 through June 11, 2019, in accordance with the DOT&E-approved test plan.
- The Lead Developmental Test Organization (LDTO), with AFOTEC participation, conducted integrated testing in four

- integrated test events from January 8 through September 26, 2018.
- The LDTO and AFOTEC jointly conducted EPS radio frequency anti-jam testing in January 2018.

# FY19 AIR FORCE PROGRAMS

- AFOTEC collected reliability, availability, and maintainability data during the dedicated operational test period and additional data from January 1 through March 24, 2019.
- The Army Threat System Management Office (TSMO) planned to conduct a 6-week persistent cyber Adversarial Assessment (AA), with strong support from the EPS Program Manager; however changing schedules and limited availability truncated the effort and caused AFOTEC to re-plan the AA events.
- TSMO conducted a Close Access Team assessment from January 14 – 18, 2019, on the EPS.
- The 47th Cyber Test Squadron performed an EPS payload cyber assessment on a payload surrogate April 10 – 12, 2019.
- The 177th Information Aggressor Squadron conducted an AA from May 14 – 18, 2019.
- Air Force Space Command accepted the EPS for military operations on September 19, 2019.

## Assessment

- Results from the MOT&E, combined with complementary integrated test data, were adequate to assess the operational effectiveness, suitability, and survivability of the EPS.
- The EPS is operationally effective in providing AEHF SATCOM XDR communications to support submarine and surface ship operations in the North Polar Region in benign and threat environments.
- Submarine communicators were able to acquire and logon to the EPS payloads, using either their mast or periscope antennas, and moved the Wide Focused Coverage Area beam over their location to send both voice and data messages.
- Ship communicators were able to acquire and logon to both EPS payloads and conduct Advanced Digital Network Communications point-to-point and Advanced Time Division Multiple Access Interface Processor communications.
- The USS *Theodore Roosevelt* (CVN 71) successfully conducted voice and data communications over EPS during the joint exercise Northern Edge 2019.
- Both ship and submarine communicators had difficulty configuring their Navy equipment properly to get it to work

over EPS. However, EPS worked well once the operators properly configured their equipment.

- When operators attempted to troubleshoot their equipment, they lacked troubleshooting guides and flowcharts.
- The help desk support for EPS communicators was inconsistent or not available. The testers often had to turn to subject matter experts from the Program Office to resolve configuration problems.
- The EPS is operationally suitable. The EPS met the user-defined operational availability and reliability requirements.
- During the testing, neither the EPS payload nor the Gateway had a critical failure. DOT&E estimates that the Mean Time Between Critical Failures (MTBCF) for these two segments is 317 percent greater than the threshold requirement. The CAPS had two critical failures that did not affect mission accomplishment.
- Both CAPS and Gateway operators felt they could use EPS to satisfy their mission requirements. Both groups felt that once trained, they were able to use EPS with ease.
- The CAPS operators thought their training and documents prepared them for their mission. The Gateway operators thought their training and documents lacked details.
- The EPS performed better than the user-defined anti-jam requirement in threat-representative testing.
- The EPS is secure from cyber-attacks from an outsider threat.

## Recommendations

The Air Force should:

1. Develop, in coordination with the Navy, an approved document that covers the end-to-end configurations, port settings, and troubleshooting flow charts for getting EPS to work with the Navy communications equipment.
2. Formalize EPS help desk procedures, including points of contacts, and publish those procedures where they are accessible to users.