# Common Submarine Radio Room (CSRR) (includes Submarine Exterior Communications System (SubECS))

**Executive Summary**
- The Navy is conducting operational testing of Increment 1 Version 2 of the Common Submarine Radio Room (CSRR) on an *Ohio* class SSGN. Testing is scheduled to be completed in FY11.
- The Navy should re-evaluate the Extremely High Frequency (EHF) communications infrastructure and system architecture in light of the increased importance of EHF communications to submarine operations. The architecture does not enable EHF communications to be re-established rapidly when interrupted.

**System**
- CSRR/Submarine Exterior Communications System (SubECS) is an umbrella program that integrates modern antennas, radios, cryptographic equipment, and messaging systems to form a submarine communications system.
- It is intended to provide a common communication system across all classes of submarines and is designed to support the steady infusion of new technology with incremental modernization and replacement of obsolete equipment.
- The program establishes common hardware and software baselines.
- *Virginia* class CSRR (designated SubECS) is developed and integrated as part of new construction. Other submarine radio rooms are being replaced with CSRR variants during maintenance periods to establish a common radio room baseline.
- The Navy intends future CSRR improvements to address obsolescence issues and add new communications capabilities as they mature.

**Mission**
The submarine Commanding Officer uses the CSRR/SubECS for communications and information dissemination in order to accomplish assigned missions. The Navy intends to use the CSRR capabilities to manage, control, and disseminate command, control, communications, computers, and intelligence information routed to and from submarines.

**Major Contractor**
Lockheed Martin Maritime Systems and Sensors – Washington, District of Columbia

**Activity**
- DOT&E approved Revision 4 to the CSRR Test and Evaluation Master Plan in December 2009. This revision addresses the FOT&E for the Increment 1 Version 2 upgrades to the baseline CSRR.
- The Navy conducted at-sea Integrated Testing of the Increment 1 Version 2 CSRR in April and May 2010. The Navy plans to complete dedicated at-sea operational testing in early FY11.
- In July 2010, the Navy issued an interim fielding decision to field Increment 1 Version 2 on three submarines (SSGN 726, SSGN 729, and SSN 23) before operational testing was complete.
- The Navy conducted an Information Assurance vulnerability evaluation of the CSRR in April 2010. The Navy plans to complete the Information Assurance testing with a penetration test of the CSRR in early FY11.
- The Navy plans to accelerate fielding of the CSRR on older *Los Angeles* class submarines, installing the first *Los Angeles* class variant in 2012 rather than 2015.

**Assessment**
- The Navy has planned adequate operational testing for Increment 1 Version 2.
- Although operational testing has not been completed, Integrated Testing results suggest that the new capabilities incorporated into Increment 1 Version 2 have been successfully installed and generally perform as expected, while the legacy capability has not been degraded.

- The Information Assurance vulnerability evaluation found that the CSRR routers are well configured to protect tactical computers. However, several computers on the CSRR network contained critical vulnerabilities and were running operating systems no longer supported by the vendor, making patching of the vulnerabilities difficult.
- The baseline CSRR adequately implements EHF, but successful EHF communications are highly dependent upon satellite availability and adequate shore support. The testers observed, and the crews reported, frequent problems conducting EHF communications. Contributing to these problems, the Navy's EHF architecture does not appear to be optimized to support rapid restoration of communications following an inadvertent interruption. In recent years, EHF connectivity has become increasingly important to submarine operations.

**Recommendations**

- Status of Previous Recommendations. The Navy has adequately addressed two of the three previous recommendations. The Navy still needs to re-evaluate the EHF communications infrastructure and system architecture so that EHF communications can be restored rapidly once interrupted.
- FY10 Recommendations. The Navy should consider:
  1. Upgrading all computers in CSRR to operating systems supported by the vendor.
  2. Instituting a comprehensive vulnerability patching process for CSRR computers that are accessible by the external network.