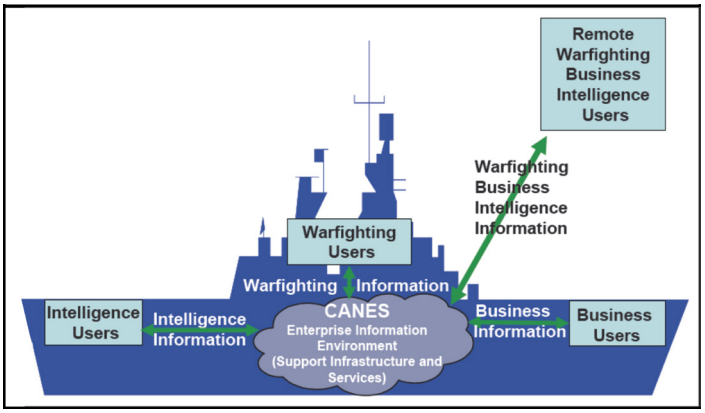
Consolidated Afloat Networks and Enterprise Services (CANES)

Executive Summary
- USD(AT&L) approved full deployment of the Consolidated Afloat Networks and Enterprise Services (CANES) on October 13, 2015, after DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable. The Commander, Operational Test and Evaluation Force (COTF) conducted IOT&E for the unit-level variant on USS *Higgins* (DDG 76) from August 2014 through March 2015.
- COTF started FOT&E of the force-level CANES variant on the USS *John C. Stennis* (CVN 74) in August 2015. COTF is working to complete the cybersecurity portion of FOT&E without affecting the Navy's mission. COTF expects to conclude cybersecurity operational testing in early 2017.
- The Navy plans to conduct an FOT&E for the submarine variant in FY19.

System
- CANES is an enterprise information system consisting of computing hardware, software, and network services (e.g., phone, email, chat, video teleconferencing, web hosting, file transfer, computational resources, storage, and network configuration and monitoring). CANES will replace legacy networks on ships, submarines, and shore sites.
- The CANES program mitigates hardware and software obsolescence on naval vessels and shore sites through the increased use of standard components and regularly scheduled hardware and software updates.
- The CANES network provides a single, consolidated physical network with logical sub-networks for Unclassified, Secret, Secret Releasable, and Top Secret security domains. It includes a cross-domain solution for information transfers across these security boundaries. This consolidation reduces the network infrastructure footprint on naval platforms and the associated logistics, sustainment, and training costs.
- CANES has three variants tailored to the employing platform: unit level for smaller ships such as destroyers and cruisers, force level for large deck ships such as aircraft carriers and large deck amphibious ships, and a submarine variant.



Mission
Naval Commanders and crew afloat and ashore use CANES to connect weapon systems, host applications, and share command and control, intelligence, and business information via chat, email, voice, and video in support of all naval and joint operations.

Major Contractors
- Northrop Grumman – Herndon, Virginia
- BAE Systems – Rockville, Maryland
- Serco – Reston, Virginia
- DRS Laurel Technologies – Johnstown, Pennsylvania

Activity
- COTF conducted the CANES IOT&E on the unit-level variant from August 2014 through March 2015.
- USD(AT&L) approved CANES full deployment on October 13, 2015, after DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable.
- COTF completed the performance and suitability testing portions of FOT&E on the force-level variant aboard USS *John C. Stennis* in August 2015, but could not complete cybersecurity testing at that time because the ship's operational schedule could not support this testing.
- COTF conducted a preliminary Cooperative Vulnerability and Penetration Assessment (CVPA) on USS *John C. Stennis* in December 2015. This test was not intended to satisfy operational testing requirements, but to identify and mitigate as many vulnerabilities as possible before the ship deployed.
- Due to the size and complexity of the force-level CANES, combined with limited ship and Red Team availability, COTF is conducting cybersecurity testing in multiple phases. The first phase focused on embarkable assets (those brought aboard by the destroyer squadron and the ship's air wing). COTF

executed this portion of the test in June 2016 while the ship was underway with the necessary units and assets.
- The test of embarkable assets included both a CVPA and Adversarial Assessment (AA).
- COTF expects to perform a CVPA for the rest of the ship in November 2016 and an AA in March 2017 pending availability of the USS *John C. Stennis* or another suitable test platform.

Assessment
- DOT&E assessed the unit level variant as operationally effective, suitable, and survivable.
- DOT&E will publish an FOT&E report on the CANES force-level variant after the completion of cybersecurity testing in FY17.

Recommendations
- Status of Previous Recommendation. The Navy is addressing the previous recommendation.
- FY16 Recommendations. The Navy should:
  1. Complete the planned cybersecurity tests for force-level ships.
  2. Continue planning the FOT&E for the submarine variant.