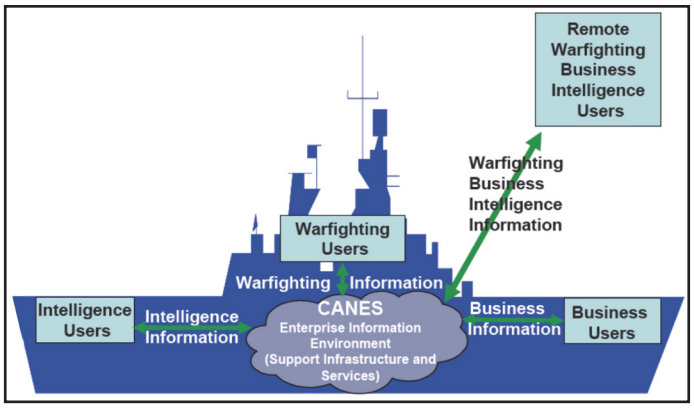
Consolidated Afloat Networks and Enterprise Services (CANES)

Executive Summary
- The Consolidated Afloat Networks and Enterprise Services (CANES) force-level variant is operationally effective and suitable, and not survivable in a cyber-contested environment, based on data from the FOT&E that ended in June 2017.
- USD(AT&L) approved full deployment of CANES on October 13, 2015, after DOT&E evaluated CANES for unit-level ships to be operationally effective, suitable, and survivable based on the data from the IOT&E.

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 is intended to 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 is intended to reduce 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 crews 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
- General Dynamics - Taunton, Massachusetts
- Serco – Reston, Virginia
- DRS Laurel Technologies – Johnstown, Pennsylvania

Activity
- The Navy's Operational Test and Evaluation Force (OPTEVFOR) completed the CANES force-level variant FOT&E in June 2017. The Navy could not execute the originally planned test schedule due to high-priority operational deployments of the designated test ships. As executed, the tests spanned from June 2015 to March 2017 on two different aircraft carriers. OPTEVFOR conducted the following events in support of the FOT&E:
  - A functional test onboard CVN 74 in August 2015.
  - A shortened Cooperative Vulnerability and Penetration Assessment (CVPA) on CVN 74 in December 2015 to identify and fix cybersecurity vulnerabilities before the ship deployed for an operational mission.
  - A second CVPA on the equipment brought onboard the CVN 74 by the air wing and destroyer squadron in June 2016.
  - The final CVPA onboard CVN 74 in November 2016, but the ship was not available for the follow-on Adversarial Assessment (AA). Normally, a cyber test team conducts a CVPA and waits until the Program Office and the user fix vulnerabilities discovered during the CVPA before conducting an AA. For this test, OPTEVFOR conducted the CVPA on CVN 74, but conducted the AA on CVN 71. The cyber test team conducted a short CVPA on CVN 71 prior to commencing the AA.

- OPTEVFOR did not conduct cybersecurity testing for the CANES Top Secret/Sensitive Compartmented Information (TS/SCI) enclave.
- As conducted, the FOT&E was adequate to evaluate operational effectiveness, operational suitability, and survivability pending cybersecurity testing of the TS/SCI enclave. DOT&E issued a report on the FOT&E on September 25, 2017.

Assessment

- The force-level CANES variant is operationally effective. CANES provides enterprise services, application hosting, network communications, and network management capabilities that support force-level missions.
- The force-level CANES variant is operationally suitable. CANES met reliability, availability, and maintainability requirements and received good usability scores. However, the Program Office should expand training and documentation to cover more topics such as monitoring the network, determining network status, assessing proposed configuration changes, and cybersecurity.
- The force-level CANES variant is not survivable. Cybersecurity vulnerabilities identified and fixed on CVN 74 still remained as vulnerabilities on CVN 71.
- The Navy does not assign a dedicated network manager on ships. A dedicated network manager with adequate cybersecurity training could monitor the network and provide the ship a means of detecting cybersecurity intrusions and taking appropriate actions.

Recommendations

- Status of Previous Recommendations. There are no outstanding previous recommendations.
- FY17 Recommendations. The Navy should:
  1. Correct all deficiencies identified in the force-level FOT&E on all Navy ships.
  2. Assign dedicated network managers on all combatant ships and provide them with cybersecurity training.
  3. Conduct cybersecurity testing of the CANES TS/SCI enclave.