Air Operations Center – Weapon System (AOC-WS)

Executive Summary

- The Air Operations Center – Weapon System (AOC-WS) 10.1 is a system-of-systems that contains numerous third-party software applications, including the Global Command and Control System – Joint (GCCS-J), Theater Battle Management Core Systems – Force Level, Master Air Attack Plan Toolkit, and Joint Automated Deep Operations Coordination System.
- The Air Force tests AOC-WS 10.1 during a three-phase Recurring Event (RE) test cycle, which includes event-based test periods primarily focused on software upgrades. The software upgrades and associated test event are designated using similar terms; for example, AOC-WS 10.1 RE13 is the system upgrade tested during RE13.
  - Phase 1 developmental testing is conducted at the Combined Air Operations Center – Experimental (CAOC-X) at Joint Base Langley-Eustis, Virginia.
  - Phase 2 operational testing is conducted to assess effectiveness at CAOC-X.
  - Phase 3 operational testing is conducted at a fielded site to assess suitability.
- In October 2015, the Air Force delivered its final report on RE13 that included the results of Phase 3 operational testing at 613 AOC, Joint Base Pearl Harbor-Hickam, Hawaii.
- AOC-WS 10.1 RE13 has the capability to produce the primary products necessary to meet the established AOC battle rhythm at threshold levels. AOC-WS 10.1 RE13 demonstrated interoperability with other mission-critical systems.
- The Air Force fully assessed cybersecurity for AOC-WS 10.1 RE13 and identified 15 vulnerabilities posing significant risk to the AOC mission, 9 of which are attributable to third-party applications that are outside the control of the AOC-WS Program Office. The first-ever Adversarial Assessment of the AOC-WS demonstrated that significant cybersecurity risk to the mission exists.
- Following the completion of Phase 3 testing at 613 AOC, there was a single Category I (CAT I) Urgent functional deficiency. Air Combat Command conducted an analysis of this deficiency and has deferred the implementation of the responsible web-based application suite during RE13 fielding until the Program Office has remediated the deficiency.
- Air Combat Command accepted the mission risk posed by the 15 identified cyber vulnerabilities, and in November 2015 decided to field AOC-WS 10.1 RE13 to meet critical operational needs, while maintaining the expectation that the AOC-WS Program Office will fix unresolved CAT I deficiencies in an expeditious manner.
- AOC-WS 10.1 RE13 is built, configured, and maintained at operational sites with the assistance of a Program Office fielding team. The site leads the build and the fielding team augments at pre-planned points during complex segment installs. Tier 1 help desk support (AOC-WS helpdesk at Joint Base Langley-Eustis) was not effective during the test, but Tier 2 (program manager/vendor support) was adequate to support the system fielding and operations during the event. Subsequent fielding events will likely depend solely on Tier 2 help desk support.

System

- AOC-WS is the senior command and control element of the U.S. Air Force's Theater Air Control System and provides operational-level command and control of air, space, and cyberspace operations, as well as joint and combined air, space, and cyberspace operations. Capabilities include command and control of joint theater air and missile defense, time-sensitive targeting, and Intelligence, Surveillance, and Reconnaissance management.
- The AOC-WS 10.1 (AN/USQ-163 Falconer) is a system of systems that contains numerous software applications developed by third party vendors and commercial off-the-shelf products. Each third-party system integrated into the AOC-WS provides its own programmatic documentation.
- The AOC-WS consists of:
  - Commercial off-the-shelf hardware
  - Separate third-party software applications, including GCCS-J, Theater Battle Management Core Systems – Force Level, Master Air Attack Plan Toolkit, and Joint Automated Deep Operations Coordination System, from which the AOC-WS draws its capabilities
  - Additional third-party systems that accept, process, correlate, and fuse command and control data from multiple sources and share them through multiple communications systems
- AOC-WS 10.1 operates on several different local area networks (LANs), including Secret Internet Protocol Router Network, Joint Worldwide Intelligence Communications System, and a coalition LAN, when required. The LANs connect the core operating system and primary applications to

joint and coalition partners supporting the applicable areas of operation. Users can access web-based applications through the Defense Information Systems Network.

- The Air Force tests AOC-WS 10.1 software upgrades during REs. The Air Force refers to each software upgrade by the RE during which it was tested. For example, AOC WS 10.1 RE13 is the software upgrade tested during RE13.
- The future AOC-WS 10.2 is designed to deliver a modernized, integrated, and automated approach to AOC WS operations.

Mission

The Commander, Air Force Forces, or the Joint/Combined Forces Air Component Commander use the AOC-WS to exercise control of joint (or combined) air forces, including planning, directing, and assessing air, space, and cyberspace operations to meet operational objectives and guidance. An operational AOC is fundamental in enabling centralized command and decentralized execution of a theater air campaign.

Major Contractors

- AOC-WS 10.1 Production Center: Jacobs Technology Inc., Engineering and Technology Acquisition Support Services – Hampton, Virginia
- AOC-WS 10.2 Modernization: Northrop Grumman – Newport News, Virginia

Activity

- The Air Force typically uses a three-phase RE test cycle for major AOC WS 10.1 upgrades, along with lower-level testing events, to sustain interoperability and cybersecurity and provide low-risk upgrades to third-party systems as required.
  - Phase 1 developmental testing is conducted at CAOC-X Joint Base Langley-Eustis, Virginia.
  - Phase 2 operational testing is conducted at CAOC-X to assess effectiveness.
  - Phase 3 operational testing is conducted at a fielded site to assess suitability.
- From March through August 2015, the Air Force conducted operational testing of AOC-WS 10.1 RE13 in accordance with the DOT&E-approved test plans. AOC-WS 10.1 RE13 intended to deliver new operational and tactical analysis capabilities, upgraded infrastructure, updated versions of third-party applications, and improved system cybersecurity posture.
- In October 2015, the Air Force completed its report on RE13, which included data from integrated testing (Phases 1 and 2) at CAOC-X, Joint Base Langley-Eustis, Virginia, in December 2014, and results from Phase 3 operational testing at 613 AOC, Joint Base Pearl Harbor-Hickam, Hawaii, from March through August 2015. Testing at the 613 AOC focused on three areas: assessing the ability of the site system administrators to correctly install, configure, and transition the AOC from the legacy AOC-WS 10.1 RE12 version to the AOC-WS 10.1 RE13 capability; validating the functional evaluation data obtained during developmental test; and assessing operational effectiveness and suitability of the upgraded system.
- In August and September 2015, AOC-WS 10.2 completed the first of two scheduled phases of developmental testing at CAOC-X. The severity and quantity of the functional and cybersecurity deficiencies identified during the test resulted in the Air Force issuing a cure notice to the prime contractor.

Assessment

- The Air Force adequately tested AOC-WS 10.1 RE13 through a combination of developmental and operational testing; however, there were significant known limitations to Reliability, Availability, and Maintainability (RAM) data.
  - Testing was conducted in accordance with the DOT&E-approved test plans, which anticipated the lack of RAM data. The duration and nature of RE13 test events provided insufficient time to allow DOT&E to assess RAM under operationally realistic system usage.
  - The Air Force has assessed that the operational tempo in fielded AOCs precludes the level of manual data collection required to support thorough RAM analysis. However, the Air Force plans to implement a technical RAM collection solution in the modernization increment, AOC-WS 10.2, which will allow DOT&E to conduct thorough analyses for future test events.
- AOC-WS 10.1 RE13 has the capability to produce the primary products necessary to meet the established AOC battle rhythm at threshold levels. AOC-WS 10.1 RE13 demonstrated interoperability with other mission-critical systems.
- The Air Force fully assessed AOC-WS 10.1 RE13 for cybersecurity, conducting the system’s first-ever Adversarial Assessment using a DOD cyber Red Team. The Cooperative Vulnerability and Penetration Assessment identified 11 vulnerabilities, 9 of which are attributable to third-party systems that could pose significant risk to the AOC-WS mission. The Adversarial Assessment identified an additional four vulnerabilities and produced associated operational effects that demonstrate significant risk to the mission exists.
- The Program Office successfully closed six of the seven functional CAT I deficiencies found during the RE13 test events. The single open RE13 CAT I functional deficiency is a result of implementing a suite of web-based applications for submitting, managing, and querying air mission reports; Intelligence, Surveillance, and Reconnaissance post-mission

summaries; and electronic warfare mission requests and reporting.

  - This deficiency affects operational suitability by requiring communications support personnel to create and maintain accounts for thousands of external users across the Services.
  - This deficiency could also affect operational effectiveness if personnel deploying to a theater were unable to establish accounts in a timely manner, or if aircrews transiting the theater without accounts were not able to submit mission reports. Both scenarios would negatively affect the ability of an AOC to conduct intelligence analysis required to accomplish mission tasks.
  - Following the completion of Phase 3 testing at 613 AOC, Air Combat Command conducted an analysis of this deficiency. The command has deferred the implementation of the web-based application suite during RE13 fielding until the Program Office has remediated the deficiency.

- Air Combat Command accepted the mission risk posed by the 15 identified cyber vulnerabilities, and decided to field AOC-WS 10.1 RE13 to meet critical operational needs, while maintaining the expectation that the AOC-WS Program Office will fix unresolved CAT I deficiencies in an expeditious manner.
- AOC-WS 10.1 RE13 can be built, configured, and maintained adequately at operational sites with Program Office-provided support during specific complex installation segments. Tier 1 help desk support was not effective for build support, but Tier 2 was adequate to support the system fielding and operations during the event. Subsequent fielding events will likely depend solely on Tier 2 help desk support.
- The key to successful testing and fielding of AOC-WS 10.1 continues to be close collaboration between the AOC-WS Program Office and the providers of third-party applications to ensure those applications meet the operational and cybersecurity needs of the AOCs. Early AOC-WS tester involvement in third-party testing continues to be necessary to identify critical problems for early corrective action.

Recommendations

- Status of Previous Recommendations. The Air Force has fully addressed one previous recommendation and has made progress towards two previous recommendations. The Air Force still needs to require AOC sites to collect and report RAM data to the Program Office. The Air Force has assessed that the operational tempo in fielded AOCs precludes the level of manual data collection required to support thorough RAM analysis. Therefore, the Air Force plans to implement a technical RAM collection solution in the modernization increment, AOC-WS 10.2, which will allow DOT&E to conduct thorough analyses for future test events.
- FY15 Recommendations. The Air Force should:
  1. Close identified cybersecurity vulnerabilities in cooperation with third-party system providers to mitigate risk to the AOC mission.
  2. Improve dynamic cyber defensive capabilities focusing on detecting and responding to cyber adversary attacks against the AOC-WS.
  3. Reassess the help desk-enabling concept to determine whether Tier 1 help desk personnel can be sufficiently trained to support the build process. For future build support, the Air Force should consider merging Tier 1 and Tier 2 functionality.