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 (TBMCS-FL), Master Air Attack Plan Toolkit (MAAPTK), and Joint Automated Deep Operations Coordination System (JADOCS).
- 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 RE12 is the system upgrade tested during RE12.
  - Phase 1 developmental testing is conducted at the Combined Air Operations Center – Experimental (CAOC-X) at Langley AFB, 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 January 2014, the Air Force delivered its final report on RE12 that included the results of Phase 3 operational testing at 612 AOC, Davis-Monthan AFB, Arizona.
- AOC-WS 10.1 RE12 has the capability to produce the primary products necessary to meet the established AOC battle rhythm at threshold levels. AOC-WS 10.1 RE12 demonstrated interoperability with other mission-critical systems. It provides a significant improvement to AOCs in both internal functionality and the ability to interoperate with respective Combatant Commands.
- AOC-WS 10.1 RE12 can be built, configured, and maintained adequately at operational sites without the assistance of a fielding team. Help desk support necessary to support the build, configuration, and maintenance of AOC-WS operations was inefficient and needs to be improved. The duration and nature of RE12 test events provided insufficient time to allow DOT&E to assess reliability, availability, and maintainability (RAM) under operationally realistic system usage.
- The legacy AOC-WS 10.1 RE11 has a valid "Authority to Operate" through November 2015. The AOC-WS Information Assurance manager determined that the RE12 update has no negative impact on the AOC-WS security posture and affirmed in a memorandum dated September 11, 2013, that the existing Authority to Operate remains valid.
- The Air Force has not yet used a DOD cyber Red Team to fully assess cybersecurity for AOC-WS 10.1 RE12. The Air Force intends to accomplish a complete cybersecurity test on AOC-WS 10.1 during RE13.

- Air Combat Command conducted a thorough analysis of the three AOC-WS 10.1 RE12 outstanding Category I (CAT I) deficiencies and accepted the risk of fielding AOC-WS 10.1 RE12 to meet critical operational needs; however, they did so while maintaining the expectation that the AOC-WS Program Office will fix those deficiencies in an expeditious manner. Two of the three CAT I deficiencies were re-identified from RE11 and one deficiency discovered was new to RE12.

System

- The 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 third-party-developed software applications 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 GCCS-J, TBMCS-FL, MAAPTK, and JADOCS, 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 area 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 event during which it was tested. For example, AOC-WS 10.1 RE12 is the software upgrade tested during RE12.
- 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 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 Langley AFB, 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.
- In August 2013, the Air Force conducted operational testing of AOC-WS 10.1 RE12. AOC-WS 10.1 RE12 incorporated Defense Information Systems Agency upgrades to GCCS-J, updates to other third-party applications, and improvements to the system's cybersecurity posture.
- In January 2014, the Air Force completed its report on RE12, which included results from Phase 2 operational testing at CAOC-X, Langley AFB, Virginia, in August 2013, and Phase 3 testing at 612 AOC, Davis-Monthan AFB, Arizona, from November through December 2013. Testing at the 612 AOC focused on the ability of the install team to correctly upgrade and configure the AOC from the legacy AOC-WS 10.1 RE11 capability to the AOC-WS 10.1 RE12 configuration, and to perform backup and recovery actions on AOC-WS 10.1 RE12.
- DOT&E submitted an Interim Assessment Memorandum on January 30, 2014, on RE12 testing observed at both CAOC-X and 612 AOC. The data from these phases of testing formed the basis for the assessment of AOC-WS 10.1 RE12's operational effectiveness and suitability.
- In 4QFY14, the Air Force commenced the AOC-WS 10.1 RE13 build at CAOC-X in anticipation of beginning RE13 testing in 1QFY15.
- In 4QFY14, AOC-WS 10.2 experienced a 3.5-month slip in schedule due to the contractor not obtaining an Interim Authority to Test. Operational testing for AOC-WS 10.2 is now scheduled to begin in November 2015.
- The Air Force conducted RE12 testing in accordance with the DOT&E-approved test plans.

Assessment

- The Air Force adequately tested AOC-WS 10.1 RE12 through a combination of developmental and operational testing; however, there were significant known limitations to cybersecurity and RAM data collection. Testing was conducted in accordance with the DOT&E-approved test plan, which anticipated the lack of RAM data. Therefore, the Air Force adopted a mitigation strategy in which they will collect and provide the required data from fielded sites, allowing DOT&E to refine the assessment results based on the ongoing analysis.
- Following the completion of Phase 3 testing at 612 AOC, Air Combat Command conducted a thorough analysis of the three outstanding CAT I Urgent deficiencies and accepted the risk of fielding AOC-WS 10.1 RE12 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. This represents a significant improvement to the 11 open CAT I deficiencies in RE11.
- RE12 successfully closed 9 of the 11 RE11 CAT I deficiencies. Of the two remaining CAT I deficiencies from RE11, one affected operational suitability and one affected cybersecurity. The third RE12 deficiency was a new deficiency, which affected operational effectiveness.
- AOC-WS 10.1 RE12 has the capability to produce the primary products necessary to meet the established AOC battle rhythm at threshold levels. AOC-WS 10.1 RE12 demonstrated interoperability with other mission-critical systems. It provides a significant improvement to AOCs in both internal functionality and the ability to interoperate with respective

Combatant Commands. Four previously documented CAT I deficiencies in RE11, which were related to GCCS-J and affected operational effectiveness, have been closed. The new RE12 CAT I deficiency relates to audio deficiencies in Defense Connect Online as deployed within the AOC-WS. This deficiency could negatively affect mission-critical coordination activities. This deficiency was not previously discovered because the operational site used a thin client configuration, whereas the developmental testing used thick clients that did not exhibit this behavior.

- AOC-WS 10.1 RE12 can be built, configured, and maintained adequately at operational sites without the assistance of a fielding team. Help desk support necessary to support the build, configuration, and maintenance of AOC-WS operations was inefficient and needs to be improved. This operational help desk was not utilized during developmental testing, and during operational testing, the help desk had to maintain both the operational system and the system under test, doubling their workload. Of the five CAT I deficiencies in RE11 affecting operational suitability, the Air Force closed all but one. The remaining deficiency is related to the inability to release Cautions, Warning, and Notes as currently written to coalition partners; this deficiency does not adversely affect U.S.-only operations.
- The duration and nature of RE12 test events provided insufficient time to allow DOT&E to assess RAM under operationally realistic system usage. The Air Force must collect additional data at operational sites to assess the effects of RAM on AOC mission operations. The Air Force plans to implement a technical RAM collection solution in the modernization increment, AOC-WS 10.2.
- The AOC-WS 10.1 RE12 test article and associated documentation that entered OT&E was the direct output of the developmental test-fix-test cycle. Time constraints precluded entering OT&E with a "clean rebuild" of the test article and a cohesive consolidation of the documentation that incorporated all the supplements (software and configuration modifications) used to "fix" the previously discovered problems. Following Phase 2 testing, the 46th Test Squadron conducted an RE12 regression build event at Eglin AFB, Florida, that validated that the build process and documentation were stable and complete prior to proceeding to Phase 3 testing at 612 AOC.
- The legacy AOC-WS 10.1 RE11 has a valid Authority to Operate through November 2015. The AOC-WS Information Assurance manager determined that the RE12 update has no negative security impact on the AOC-WS security posture and affirmed in a memorandum dated September 11, 2013, that the existing Authority to Operate remains valid.
- The Air Force has not yet fully assessed AOC-WS 10.1 RE12 for cybersecurity. AOC-WS 10.1 RE12 and recurring periodic software patches should significantly improve the cybersecurity posture of the system. The Air Force intends to accomplish a complete cybersecurity test on AOC-WS 10.1 during RE13.
- The key to successful testing and fielding of AOC-WS 10.1 continues to be closer collaboration between the AOC-WS Program Office and Defense Information Systems Agency to ensure GCCS-J meets the operational needs of the AOCs. Early AOC-WS tester involvement in GCCS-J testing continues to identify critical problems early for corrective action.

Recommendations

- Status of Previous Recommendations. The Air Force has made progress in addressing the remaining two previous recommendations; however, cybersecurity testing needs improvement and still needs to be addressed. Over the past two years, the Air Force has increased its efforts with two long-term FY11 recommendations (below), and this engagement needs to continue.
  1. Coordinate with third-party programs to ensure that critical AOC-WS third-party systems (such as GCCS-J) have testable requirements that meet AOC-WS requirements. The requirements should be vetted within the appropriate user and program communities for schedule and funding priority.
  2. Ensure the AOC-WS users and test community continue to actively participate in GCCS-J developmental and operational testing and collaborate to develop a capability to adequately test GCCS-J to AOC-WS threshold stress levels.
- FY14 Recommendations. The Air Force should:
  1. Improve the procedures and implementation of help desk support to operational units fielding AOC-WS 10.1 RE12.
  2. Conduct an assessment of operational risk to the AOC warfighting mission using DOD cyber Blue and Red Teams in an operationally realistic environment, consistent with DOT&E cybersecurity testing procedures.
  3. Require operational AOC sites to collect and report all significant RAM data to the Program Office, assess the data for needed system improvements, and report on RAM improvement efforts monthly to the Configuration Review Board. DOT&E will continue to review RAM data periodically and adjust our findings in accordance with this analysis.