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 incorporates third-party software applications, to enable its mission execution.
- In October and November 2015, the Air Force conducted an assessment of Out-of-Cycle (OOC) 13.1 at Combined Air Operations Center – Experimental (CAOC-X).
  - OOC 13.1 was found to be not operationally effective due to three Category I deficiencies.
  - Resolution of the Category I deficiencies was scheduled to be accomplished in OOC 13.3 in November and December 2016; however, the Defense Information Systems Agency (DISA) failed to provide the Program Management Office with viable updates.
  - OOC 13.1 was found to be operationally suitable, and there were no significant cybersecurity findings.
  - The AOC Configuration Review Board (CRB) has recommended fielding OOC 13.1 despite the Category I deficiencies in order to meet other warfighter capability requirements.
- In February 2016, the Air Force conducted an assessment of OOC 13.2 at CAOC-X.
  - OOC 13.2 was found to be operationally effective and suitable, but one portion of software content introduced four Category II cybersecurity deficiencies. The Air Force removed the non-secure content from the delivery, deferring fielding until the four deficiencies are resolved.
  - The CRB approved fielding of OOC 13.2 in conjunction with the fielding of OOC 13.1, since its implementation requires a successful OOC 13.1 installation.
- AOC-WS 10.2 failed to complete a second round of developmental testing and the associated operational assessment activities.
  - The test was canceled at the half-way point due to the number and severity of deficiencies identified.
  - The program is now proceeding through a Critical Change Review.

System

- The AOC-WS 10.1 (AN/USQ-163 Falconer) is a system of systems that incorporates 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
  - Software—including Theater Battle Management Core Systems – Force Level and Master Air Attack Plan Toolkit—to enable planning, monitoring, and directing the execution of air, space, and cyber operations

  - Third-party software applications—including Global Command and Control System – Joint (GCCS-J) and Joint Automated Deep Operations Coordination System—to enable joint and interagency integration
  - Additional third-party systems that accept, process, correlate, and fuse command and control data from multiple sources and share them through multiple communications systems
  - Voice, digital, and data communications hardware
- AOC-WS 10.1 operates on several different local area networks (LANs), including the 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 typically tests major functionality upgrades to AOC-WS 10.1 during a three-phased Recurring Event (RE) test cycle, which includes event-based test periods primarily focused on software upgrades. The three phases of the RE test cycle typically includes:
  - Phase 1: Developmental testing conducted at the CAOC-X located at Joint Base Langley-Eustis, Virginia.
  - Phase 2: Operational testing conducted at CAOC-X to assess effectiveness.
  - Phase 3: Operational testing conducted at a fielded site to assess suitability.
- Testing of lower level, minor functionality upgrades, with assessment of "operational processes," are integrated with the latter portions of developmental testing. For these minor functionality upgrades (as opposed to purely cybersecurity

updates or maintenance-type upgrades), the Air Force uses the term OOC for their testing; i.e. OOC 13.1.

- The future upgrade, AOC-WS 10.2, is designed to deliver a modernized, integrated, and automated approach to AOC operations.
- Command and Control Air Operations Suite-Command and Control Information Services (C2AOS-C2IS) is a software developmental program to upgrade critical AOC-WS mission software, enhancing the ability of operators to perform AOC core tasks more quickly and efficiently, as well as providing new planning and execution capabilities for integrated air and missile defense and net-enabled weapons.

Mission

- The Commander, Air Force Forces or the Joint/Combined Forces Air Component Commander uses 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.
- The AOC is the senior command and control element of the Air Force's Theater Air Control System and provides operational-level command and control of joint and combined air, space, and cyberspace operations. The AOC's capabilities include command and control of joint theater air and missile defense; preplanned, dynamic, and time-sensitive multi-domain target engagement operations; and intelligence, surveillance, and reconnaissance operations management.

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

- In October and November 2015, the Air Force conducted operational testing of AOC-WS 10.1 OOC 13.1 in accordance with the DOT&E-approved test concept briefing and test plans. The primary focus of OOC 13.1 was to upgrade GCCS-J from version 4.2.0.9U2 to version 4.3U1. This upgrade of GCCS-J also required compatibility updates to the Joint Automated Deep Operations Coordination System and Theater Battle Management Core Systems.
- In February 2016, the Air Force conducted operational testing of AOC-WS 10.1 OOC 13.2 in accordance with the DOT&E-approved test concept briefing and test plans. The objectives of OOC 13.2 were to improve the AOC-WS' cybersecurity posture by closing over 200 Category II open deficiencies, upgrading the Master Air Attack Plan Toolkit, adding a Microsoft® active directory users and computer console (ADUC), and upgrading the Airspace Management Application.
- In April 2016, the Air Force completed its reports on OOC 13.1 and OOC 13.2. Both reports included data from integrated testing at CAOC-X.
- In August 2016, the AOC CRB recommended fielding OOC 13.1 and OOC 13.2 because GCCS-J 4.3U1, despite its deficiencies, is a better product than the currently fielded GCCS-J 4.2.0.9U2. The CRB made this decision because DISA failed to deliver a viable update to GCCS-J 4.3U1 that can be integrated into the OOC 13.3 to address OOC 13.1's Category I deficiencies.
- In February and March 2016, AOC-WS 10.2 failed to complete the second of two scheduled phases of developmental testing at CAOC-X. These failures occurred after contractor remediation actions taken as a result of Cure Notices issued in September 2014 and September 2015. A Cure Notice is a letter from the government to the contractor regarding concerns about poor performance in accordance with contract requirements. The severity and quantity of the functional and cybersecurity deficiencies identified during the first half of developmental testing resulted in the cancelation of the remaining developmental test events and planned operational assessment activities. Currently, the program is conducting a Critical Change Review.
- In June and July 2016, the Air Force conducted early developmental testing on several C2AOS-C2IS capability packages. These and subsequent developmental test events are precursors to integrating all the capability packages into a single software release that will be integrated into the AOC-WS baseline and then undergo IOT&E.

Assessment

- The Air Force adequately tested AOC-WS 10.1 OOC 13.1 and OOC 13.2 with an assessment of operational processes during integrated developmental/operational test events.
- OOC 13.1 was found to be not operationally effective due to three open Category I deficiencies against third-party software that affect AOC operations in two critical ways:
  - No acceptable public key infrastructure-enabled user authentication capability, which is required for access to GCCS-J integrated imagery and intelligence applications.
  - Due to the excessive track clutter that results in an unusable common operational picture (COP) display, operators are unable to monitor and assess electronic warfare threats. In addition, there is insufficient source information to enable COP managers to resolve these track clutter problems.
- Initially, OOC 13.1 was found to be operationally suitable with limitations. The upgrade could not be conducted without extensive Tier 2 Help Desk direct onsite interaction with the build team. However, subsequent software supplements and

improved build documentation resolved the issues, improving the assessment to operationally suitable.

- A cybersecurity evaluation of OOC 13.1 resulted in no significant findings and concluded that the results from RE13 (completed in August 2015) remain valid. However, the OOC 13.3 test concept includes a full Cooperative Vulnerability and Penetration Assessment of the OOC 13.1 functional capabilities along with the OOC 13.3 upgrades and fixes, and should provide an updated assessment of the baseline cybersecurity posture.
- OOC 13.2 was found to be operationally effective and suitable. During testing, four Category II cybersecurity deficiencies associated with ADUC increased the risk to the AOC-WS baseline. Consequently, the Air Force removed ADUC from OOC 13.2 until the deficiencies can be resolved, targeting ADUC for incorporation into RE15. Additionally, since OOC 13.2 cannot be implemented without the successful installation of OOC 13.1, its fielding was delayed while the Air Force attempted to resolve the OOC 13.1 issues.
- Air Combat Command initially decided not to field OOC 13.1 until the Category I deficiencies are fixed. Resolution of the Category I deficiencies was scheduled to be accomplished in OOC 13.3 in November and December 2016; however, DISA failed to provide the Program Management Office with viable updates. Therefore, despite the Category I deficiencies, the AOC CRB recommended fielding OOC 13.1, along with OOC 13.2, beginning in September 2016. These would enable delivery of upgraded capabilities to meet other warfighter operational requirements. Resolution of OOC 13.1 deficiencies are planned to be delivered as part of RE15, scheduled to be tested in April and May 2018.
- 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 AOC. 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 made progress on one FY15 recommendation by developing and testing software updates that close cybersecurity vulnerabilities. However, the more secure software has not yet been deployed because of operational deficiencies, and new deficiencies have been identified with third-party software. The Air Force still needs to address the FY15 recommendations to improve dynamic cyber defensive capabilities focused on detecting and responding to cyber-attacks against the AOC-WS, and to reassess the Help Desk-enabling concept to support the build process. Additionally, the Air Force still plans to address a long-standing requirement to collect and report reliability, availability, and maintainability (RAM) data to the Program Office and DOT&E by implementing a technical RAM collection solution in the modernization increment, AOC-WS 10.2.
- FY16 Recommendations. None.