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 numerous software applications to conduct operational command and control (C2) of theater air, space, and cyber operations.
- In November and December 2016, the Air Force conducted an assessment of AOC-WS 10.1.13.3 to evaluate corrections to previously identified AOC-WS software discrepancies, upgrade AOC-WS management and mission application software, and advance the AOC-WS cybersecurity posture.
- In April and May 2017, the Air Force conducted an assessment of AOC-WS 10.1.14.E to evaluate improved encrypted access for mission software, upgrade monitoring and management capabilities of AOC systems, and advance the AOC-WS cybersecurity posture.
- Most of the contents of AOC-WS 10.1.13.3 and AOC-WS 10.1.14.E demonstrated the required capabilities for the AOC to execute the joint air tasking order cycle and conduct operational C2 of theater air operations.
  - Cybersecurity evaluations of both upgrades revealed vulnerabilities that pose risks to the AOC-WS contribution to mission.
  - To assure continued AOC Intelligence, Surveillance, and Reconnaissance Division (ISRD) contribution to the mission, the AOC-WS should maintain the Image Product Library (IPL) until Information Storage (iSToRE) can replicate all required legacy capabilities and correct known deficiencies.
  - Theater Battle Management Core Systems (TBMCS) testing identified incompatibility between TBMCS and the Air Support Operations Center. This was documented as a critical Category I deficiency.
- Despite the known cybersecurity vulnerabilities and the existing TBMCS Category I deficiency, Air Combat Command (ACC) elected to field both upgrades. The Air Force decided the operational gain of fielding TBMCS' new cryptographic-controlled access for all users and other operational capability gains in both upgrades outweighed the risk to mission.
- In April 2017, after the Senate Armed Services Committee denied the Air Force request for AOC-WS 10.2 program funding, the Air Force ceased contracted efforts on AOC-WS 10.2 development.
  - In October 2016, the Air Force submitted a Critical Change Report (CCR) after the program failed to meet Milestone C requirements and Full Deployment Decision within the 12-month program estimates for the second time.
  - The CCR was informed by poor capability performance during developmental testing.
- In August 2017, the Air Force canceled the AOC-WS 10.2 contract and is pursuing alternative approaches to achieve faster development, testing, and fielding of AOC-WS 10.2 requirements.

System

- The AOC-WS 10.1 (AN/USQ-163 Falconer) is a system of systems that incorporates numerous third-party software applications and commercial off-the-shelf products. Each third-party system integrated into the AOC-WS provides its own programmatic documentation.
- AOC-WS capabilities include C2 of joint theater air and missile defense; pre-planned, dynamic, and time-sensitive multi-domain target engagement operations; and intelligence, surveillance, and reconnaissance operations management.
- The AOC-WS consists of:
  - Commercial off-the-shelf voice, digital, and data communications hardware
  - AOC-WS software
  - Some software, including TBMCS – Force Level and the Master Air Attack Plan Toolkit (MAAPTK), is developed specifically for the AOC-WS to enable planning, monitoring, and directing the execution of air, space, and cyber operations
  - Other software applications, including Global Command and Control System – Joint (GCCS-J) and the Joint Automated Deep Operations Coordination System, are used by the AOC-WS to enable joint and interagency integration
  - Additional third-party systems that accept, process, correlate, and fuse C2 data from multiple sources and share them through multiple communications systems
- When required, the AOC-WS operates on several different local area networks (LANs), including the SECRET Internet Protocol Router Network, Joint Worldwide Intelligence Communications System, and a coalition LAN. 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 AOC-WS 10.2 requirements for a modernized, integrated, and automated approach to AOC operations remain valid. Following the cancellation of the AOC-WS 10.2 program, the Air Force remains committed to developing and fielding modernized AOC capabilities.
- C2 Air Operations Suite – C2 Information Services (C2AOS-C2IS) is a software developmental program to upgrade critical AOC-WS mission software. The Air Force intends to use the C2AOS-C2IS to enhance the ability of operators to perform AOC core tasks quickly and efficiently, as well as provide 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 C2 of joint (or combined) air forces, including planning, directing, and assessing air, space, and cyberspace operations; air defense; airspace control; and coordination of space and mission support not resident within theater.

Major Contractors

- AOC-WS 10.1 Production Center: Raytheon Intelligence, Information and Services – Dulles, Virginia
- AOC-WS 10.2 Modernization: Northrop Grumman – Newport News, Virginia

---

Activity

- In November and December 2016, the Air Force conducted an assessment of the AOC-WS 10.1.13.3, which included a Cooperative Vulnerability Inspection (CVI). The Operational Test Agency, 605th Test and Evaluation Squadron (TES), approved the test plan in accordance with delegated authority in DOT&E policy memo, "Guidelines for OT&E of Information and Business Systems," September 14, 2010. To support agile acquisition and fielding approaches, DOT&E delegates test plan approval based on an assessment of moderate or low overall risk to mission accomplishment of new software integration. AOC-WS 10.1.13.3 was assessed as moderate risk. The focus of this upgrade was to correct previously identified software discrepancies, upgrade AOC-WS management software, and advance the AOC-WS cybersecurity posture.
  - The AOC-WS software upgrades included GCCS-J, MAAPTK, and TBMCS – Force Level.
  - Additionally, this AOC WS upgrade added iSToRE software as a replacement for the AOC ISRD IPL software.
- In April and May 2017, the Air Force conducted an assessment of the AOC-WS 10.1.14.E, which included a CVI. AOC-WS 10.1.14.E new software integration was assessed as moderate risk to mission accomplishment. 605 TES approved the test plan in accordance with delegated authority from DOT&E. The focus of this upgrade was to advance the cybersecurity posture of AOC-WS; improve encrypted access for TBMCS and GCCS-J; upgrade AOC-WS software applications; and improve the capability to monitor and manage user computer-based access to AOC systems.
- In April 2017, after completion of the 2016 CCR, the Senate Armed Services Committee did not approve the Air Force budget request for AOC-WS 10.2. In August 2017, the Air Force ceased contracted efforts on AOC-WS 10.2 development and terminated the AOC-WS 10.2 contract. The Air Force stated that the current traditional acquisition strategy was not suited to take advantage of industry best practices for software development to quickly develop and field AOC-WS 10.2 requirements.
- In accordance with DOT&E recommendations, the Air Force is planning a comprehensive cybersecurity evaluation during the AOC-WS 10.1.15 upgrade planned for FY18.

Assessment

- During the November to December 2016 integrated developmental and operational test events, the Air Force adequately tested AOC-WS 10.1.13.3.
  - AOC-WS 10.1.13.3 demonstrated the required capabilities for the AOC to execute the joint air tasking order cycle and conduct operational C2 of theater air operations. While the Air Force identified some functional deficiencies during testing, these should not significantly affect the operational effectiveness and suitability of AOC-WS.
  - While iSToRE enhanced ISRD imagery management capabilities, it did not replace all the legacy functionality that currently exists in IPL.
  - A cybersecurity evaluation of AOC-WS 10.1.13.3 revealed vulnerabilities that pose risks to the AOC-WS mission.
  - In April 2017, despite the known cybersecurity vulnerabilities and some functional deficiencies, the AOC Configuration Review Board elected to field the AOC-WS 10.1.13.3 upgrade. The Air Force decided the gain in operational capability outweighed the possible risks to mission.
- During the April to May 2017 integrated developmental and operational test events, the Air Force adequately tested AOC-WS 10.1.14.E.
  - With one exception, AOC-WS 10.1.14.E demonstrated the required capabilities to support AOC execution of the joint air tasking order cycle and to conduct operational C2 of theater air operations.

- Previous TBMCS testing identified an incompatibility between TBMCS and the Air Support Operations Center. The interface incompatibility was documented as a critical Category I deficiency.
- A cybersecurity evaluation of AOC-WS 10.1.14.E revealed vulnerabilities that pose risks to the AOC-WS mission.
- In September 2017, despite the known cybersecurity vulnerabilities and existing Category I functional deficiency, ACC elected to accept the mission risk and field the AOC-WS 10.1.14E upgrade. The Air Force decided the operational gain of fielding TBMCS' new cryptographic controlled access for all users and other operational capability gains in AOC-WS 10.1.14.E outweighed the risk to the mission.

Recommendations

- Status of Previous Recommendations. The Air Force made progress on one FY15 recommendation by developing and testing software updates that close previously identified cybersecurity vulnerabilities. However, the Air Force faces the ongoing challenge of addressing emerging cybersecurity vulnerabilities identified in each AOC-WS upgrade, some of which are associated with third-party software not controlled by the AOC-WS Program Office. To address the FY15 recommendations, the Air Force needs to:
  1. Continue to improve AOC-WS dynamic cyber threat defense capabilities.
  2. Reassess the Help Desk Enabling Concept to support the installation and fielding of new capabilities at operational AOC locations.
- FY17 Recommendations. The Air Force should:
  1. Enable the AOC-WS to maintain IPL until iSToRE can replicate all required legacy capabilities and correct known deficiencies to assure continued ISRD contribution to mission.
  2. Collaborate with OSD to identify and implement any innovative operational test approaches to support the agile software development and fielding of future AOC-WS capabilities.
  3. Based on the cancellation of the AOC-WS 10.2 upgrade program, implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.