# Air Operations Center – Weapon System (AOC-WS)

## Executive Summary

- The Air Force canceled the Air Operations Center – Weapon System (AOC-WS) 10.2 contract in July 2017 and program in January 2018. In July 2018, the Air Force authorized alternative approaches via National Defense Authorization Act Section 804, Middle Tier Acquisitions, to achieve faster development, testing, and fielding of AOC-WS 10.2 requirements.
- From October 2017 through July 2018, the Air Force conducted developmental and operational test of AOC-WS 10.1 Release 10.1.15, which included a cybersecurity Cooperative Vulnerability and Penetration Assessment (CVPA).
- In July 2018, the Air Force authorized the use of Section 804 for Command and Control (C2) Air Operations Suite – C2 Information Services (C2AOS C2IS) to deliver a Minimum Viable Product (MVP) via the AOC-WS Modifications "Block 20" effort executed by the Air Force Kessel Run organization. The Air Force intends to transition the program to AOC-WS Modifications "Block 20" for continued modernization and sustainment.
- The AOC Configuration Review Board conducted a Full Deployment Decision of AOC-WS 10.1 Release 10.1.15 in September 2018.

## 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 software and hardware for voice, digital, and data communications infrastructure.
  - Government software applications developed specifically for the AOC-WS to enable planning, monitoring, and directing the execution of air, space, and cyber operations to include:
    - Theater Battle Management Core Systems (TBMCS) – Force Level
    - Master Air Attack Plan Toolkit (MAAPTK)
  - Other government software applications used by the AOC-WS to enable joint and interagency integration include:
    - Global Command and Control System – Joint (GCCS-J)
    - Joint Automated Deep Operations Coordination System (JADOCS)

  - 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 networks, including the SIPRNET, Joint Worldwide Intelligence Communications System, and coalition networks. The networks connect the core operating system and primary applications to joint and coalition partners.
- The AOC-WS 10.2 requirements for a modernized, integrated, and automated approach to AOC operations remain valid.
- C2AOS C2IS is a software developmental program to upgrade critical AOC-WS mission software, including TBMCS. The Air Force intends to deliver an MVP via the AOC Modifications "Block 20."

## 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 Modifications "Block 20" (Section 804): Raytheon Intelligence, Information and Services – Dulles, Virginia; Pivotal Software, Inc. – San Francisco, California
- C2AOS-C2IS (Section 804): Leidos – Reston, Virginia; Pivotal Software, Inc. – San Francisco, California

## Activity

- From October 2017 through July 2018, the Air Force conducted operational test of AOC-WS 10.1 Release 10.1.15, which included a cybersecurity CVPA. DOT&E approved the test plan submitted by the Operational Test Organization, the 605th Test and Evaluation Squadron (TES).
  - Release 10.1.15 updates software applications including GCCS-J, MAAPTK, and TBMCS – Force Level.
  - Additionally, Release 10.1.15 updates hardware and software providing core services, to include privileged SIPRNET tokens, virtualized servers, and updated server and workstation operating systems.
  - The Air Force delayed the execution of the cybersecurity Adversarial Assessment (AA) scheduled for July 2018, as described in the DOT&E-approved test plan, due to schedule conflicts with the 177th Information Aggressor Squadron. The 605 TES completed the AA in November 2018, evaluation and reporting are in progress.
- In September 2018, despite the known cybersecurity vulnerabilities and functional deficiencies, the AOC Configuration Review Board elected to field AOC-WS 10.1 Release 10.1.15.

## Assessment

- The Air Force adequately tested Release 10.1.15 during integrated developmental and operational test.
- Release 10.1.15 demonstrated the required capabilities for the AOC to execute the joint air tasking order cycle and conduct operational C2 of theater air operations. AOC-WS is operationally effective.
- The 605 TES identified two new Category I functional deficiencies during test. AOC-WS is not operationally suitable, primarily because of these Category I deficiencies. Additionally, the Air Force has not developed a plan to collect and report reliability, availability, and maintainability data.
- The integrated test and CVPA of Release 10.1.15 revealed new Category I deficiencies in this update that degrade the survivability of the AOC. Details are classified.

## Recommendations

The Air Force should:

1. Fix or mitigate the Category I cybersecurity and functional deficiencies in AOC-WS 10.1 Release 10.1.15.
2. Implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.