Air Operations Center – Weapon System (AOC-WS)

Executive Summary

- The USD(AT&L) canceled the Air Operations Center – Weapon System (AOC-WS) 10.2 program in 2018.
- Part of the AOC-WS 10.2 program was the Command and Control (C2) Air Operations Suite – C2 Information Services (C2AOS-C2IS).
- In July 2018, the Air Force Program Executive Officer (PEO) Digital transitioned C2AOS-C2IS to a middle tier of acquisition (MTA) rapid prototyping effort under the AOC-WS Modifications "Block 20" program.
- In March 2019, PEO Digital concluded the C2AOS-C2IS program MTA rapid prototyping effort.
- AOC-WS "Block 20" capabilities are being developed by the Kessel Run Experimentation Lab (KREL); an organic Air Force software development MTA effort.

System

- The AOC-WS (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
  - 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.
- AOC-WS 10.2 was a program designed to upgrade legacy 10.1 capabilities with a modernized, integrated, and automated approach to AOC operations.
- USD(AT&L) canceled the AOC-WS 10.2 program in 2018. The AOC-WS 10.2 requirements remain valid.
- A subset of the AOC-WS 10.2 program was the C2AOS-C2IS program. C2AOS-C2IS was a software developmental program to upgrade critical AOC-WS mission software, including TBMCS.
- PEO Digital intends to deliver these capabilities via the MTA AOC Modifications "Block 20" program. The Air Force's organic KREL software development organization focuses on this effort.

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): Air Force KREL – Boston, Massachusetts; Pivotal Software, Inc – Washington, D.C.

Activity

- In November 2018, the 605th Test and Evaluation Squadron (TES) completed the Adversarial Assessment (AA) of AOC-WS 10.1 Release 10.1.15 in accordance with the DOT&E-approved test plan. DOT&E published the classified AOC-WS 10.1 Release 10.1.15 final report in May 2019.
  - 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.
  - No cybersecurity assessments have been conducted on the "Block 20" Modification program.
- After the deployment of AOC-WS 10.1 Release 10.1.15, the AOC-WS 10.1 program transitioned to an Agile Release Event (ARE) construct. In October 2018, 605 TES started development of a Continuous Risk Assessment (CRA) process to support the ARE process. DOT&E was able to monitor and approve the CRA for the first time in October 2019. Five AREs have been released since the transition.
- PEO Digital transitioned the C2AOS-C2IS requirements to an MTA rapid prototyping program in July 2018. Then, in March 2019, PEO Digital concluded the MTA rapid prototyping program.
- The AOC-WS 10.2 requirements, including the former C2AOS-C2IS capabilities, such as TBMCS and MAAPTK, are now dispersed among five portfolios in the Kessel Run MTA Air Operations Branch: Allocations, Taskings, and Re-tasking; Data Science; Intelligence Collection; Objectives, Monitoring, and Assessments; and Target Development.
- The 47th Cyberspace Test Squadron completed an initial discovery and limited assessment of the KREL in June 2019, and published a classified report of the cybersecurity vulnerabilities in July 2019.
- The Air Force has not updated the 2011 Test and Evaluation Master Plan (TEMP) or applicable test plans to reflect the new processes.

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 AA for AOC-WS Release 10.1.15 identified new Category I deficiencies that degrade the survivability of the AOC. DOT&E published a classified Final Report in May 2019.
- The Air Force has not developed a plan to collect and report reliability, availability, and maintainability data.

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. Submit a TEMP and applicable test plans for DOT&E approval that reflects the MTA rapid fielding process.
3. Implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.