Air Operations Center – Weapon System (AOC-WS)

Executive Summary

- The Air Force's Kessel Run Experimentation Lab (KREL) is developing and deploying Air Operations Center – Weapon System (AOC-WS) Block 20 software to the field. The Air Force intends to conduct full operational testing once the aggregate Block 20 capability is sufficient to replace the currently-fielded AOC-WS 10.1.
- The Air Force's limited cybersecurity assessment of KREL demonstrated good cybersecurity processes, and identified risks to the mission. Additional cybersecurity testing is required for an adequate assessment.

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 Command and Control (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 Air Force Life Cycle Management Center (AFLCMC), Detachment 12, at Hanscom AFB, Massachusetts, is responsible for the development and sustainment of both AOC-WS 10.1 and Block 20.
- 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:
    - 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 Block 20 is a middle tier of acquisition (MTA) program intended to replace AOC-WS 10.1 with modernized, integrated, automated, and redundant capabilities to meet valid requirements defined for the previously canceled AOC-WS 10.2 program. The AOC-WS Block 20 enterprise is envisioned to consist of:
  - Operational AOCs using Block 20 infrastructure and software applications.
  - The AFLCMC, Detachment 12's organic KREL software factory developing the new applications.
  - Detachment 12's U.S. East Coast unit at Langley, AFB, Virginia, coordinating the delivery of Block 20 infrastructure and KREL-developed applications to the AOCs, providing sustainment and help desk capabilities, and enabling continuity of operations procedures.

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 Block 20 (Section 804): AFLCMC KREL – Boston, Massachusetts; Pivotal Software, Inc. – Washington, D.C.

Activity

- Substantial coronavirus (COVID-19) pandemic restrictions, such as limits to travel, access to facilities, and access to planning and analysis systems contributed to delays and limitations to cybersecurity testing of AOC-WS 10.1 and Block 20.

- The Air Force's KREL is developing and deploying AOC-WS Block 20 software to the field. The Air Force intends to conduct full operational testing when the aggregate Block 20 capability is sufficient to replace the currently-fielded AOC-WS 10.1.
- The AOC-WS 10.1 program used an Agile Release Event (ARE) construct to test and field capability updates. The 605th Test and Evaluation Squadron (605 TES) tested four AREs during FY20 (AREs 19-10, 20-02, 20-06, and 20-10). The 605 TES used a continuous risk assessment (CRA) process to determine the level of test for each ARE and then requested DOT&E review and concurrence.
- The Air Force has not performed operational cybersecurity testing on any of the eight AREs conducted since October 2018.
- In February 2020, and again in June 2020, DOT&E directed the program to accomplish full cybersecurity testing on AOC-WS 10.1 at an operational AOC to determine and mitigate cybersecurity risks to the system.
- DOT&E determined the ARE 20-06 upgrade required an operational utility evaluation with representative users operating the system to identify and mitigate possible deficiencies. The Air Force assessed the risk to test personnel conducting operational testing in a COVID-19 environment as unacceptable and decided to field ARE 20-06 without operational testing. The Air Force anticipates future testing at the first install site and each subsequent install to reduce associated risk.
- The Air Force Operational Test and Evaluation Center (AFOTEC) conducted a limited cybersecurity adversarial assessment (AA) of KREL to assess mission risks and cyber defenses of the software factory and to obtain sufficient data on the factory's systems, networks, and processes to facilitate the development of a T&E strategy for the AOC-WS enterprise. AFOTEC conducted testing in August 2020, consistent with the DOT&E-approved test plan. Due to known test limitations on data collection and threat emulations, additional cooperative and adversarial events are necessary. AFOTEC's AA test and analysis were delayed and conducted in a remote environment due to COVID-19 restrictions.
- The 47th Cyberspace Test Squadron completed two cooperative vulnerability identification cybersecurity developmental tests on KREL and issued classified reports in November 2019 and June 2020. They also completed a congressionally mandated assessment of the AOC-WS enterprise in September 2020, with a classified report to follow once analysis is complete.
- AFOTEC provided DOT&E a draft Over-Arching Test Plan for AOC-WS Block 20 that proposes collecting operational data on individual applications via all means available to include remotely, via direct observation at KREL, and in concert with developmental testers. This aligns with DOT&E initiatives to use all test venues and assets to accomplish operationally relevant testing as soon as practical during system program development. However, the Air Force has not updated the 2011 Test and Evaluation Master Plan (TEMP) to reflect the new MTA processes.

Assessment

- The AFOTEC AA cybersecurity testing of the KREL identified risks to the KREL mission as well as disciplined defensive capabilities. DOT&E expects to issue a report in 2QFY21, once the analysis is complete.
- The Air Force adequately tested three AREs (19-20, 20-02, 20-06) in October 2019, February 2020, and June 2020 for operational effectiveness and suitability.
- The Air Force has not developed a plan to collect and report reliability, availability, and maintainability data.

Recommendations

The Air Force should:

1. Conduct adequate cybersecurity testing of both AOC-WS 10.1 and the AOC-WS Block 20 enterprise to assess current risks to AOC missions and support prioritization of remediation efforts.
2. Evaluate the cybersecurity posture of AOC-WS 10.1 as modified by eight successive AREs.
3. Submit a TEMP and applicable test plans for DOT&E approval that reflect the MTA rapid fielding process.
4. Implement a solution to meet the long-standing requirement to collect and report reliability, availability, and maintainability data for the AOC-WS.