Battle Control System – Fixed (BCS-F)

Executive Summary
- In June 2017, the Air Force completed a Force Development Evaluation (FDE) on the Battle Control System – Fixed (BCS-F) Increment 3, Release 3.2.4 (R3.2.4) at all U.S. Air Defense Sectors (ADSs) and Regional Air Operations Centers (RAOCs).
- Planned BCS-F R3.2.4 capabilities included:
  - Corrections to known system management software deficiencies
  - An upgraded Radiant Mercury Guard information exchange security software and hardware
  - An upgraded cybersecurity intrusion detection system and firewall capabilities
  - Upgraded capabilities for managing information and data exchanges
  - An improved system cybersecurity posture
- While the Air Force identified some deficiencies, the ADSs and RAOCs equipped with BCS-F R3.2.4 were able to use operator workarounds to execute command and control and air battle management to support air sovereignty and air defense operations.
- As of August 2017, the Air Force transitioned to operational employment of BCS-F R3.2.4 at all ADSs and RAOCs.

System
- BCS-F is the tactical air surveillance and battle management command and control system for the continental U.S. and Canadian ADSs (Eastern ADS, Western ADS, Alaska RAOC, Canadian ADS) of the North American Aerospace Defense Command (NORAD) and U.S. Pacific Command (USPACOM) Hawaii RAOC.
- The system utilizes commercial off-the-shelf hardware within an open-architecture software configuration and operates within the NORAD and USPACOM air defense architecture.
- BCS-F integrates with the Federal Aviation Administration (FAA) via reception of FAA air surveillance radar and aircraft flight plan information.
- BCS-F R3.2.4 is a software and hardware sustainment upgrade of the BCS-F Increment 3. BCS-F R3.2.4 provides system management software upgrades, but does not add any new operational capabilities. The BCS-F R3.2.4 upgrade continues system sustainment improvements in preparation for integration with the new Wide Area Surveillance (WAS) sensor and an updated cybersecurity operational evaluation. BCS-F R3.2.4:
  - Replaced system cybersecurity intrusion detection and firewall hardware and software
  - Upgraded the Radiant Mercury Guard information exchange software and hardware
  - Upgraded system cybersecurity capabilities for managing information and data exchanges
  - Advanced the BCS-F cybersecurity posture

Mission
- The Commander, NORAD and Commander, USPACOM use BCS-F to execute command and control and air battle management to support air sovereignty and air defense missions for North American Homeland Defense and USPACOM air defense.
- Air defense operators employ BCS-F to conduct surveillance, identification, and control of U.S. sovereign airspace and control air defense assets, including fighters, to intercept and identify potential air threats to U.S. airspace.

Major Contractor
Raytheon Systems – Fullerton, California

Activity
- From April through June 2017, the 605th Test and Evaluation Squadron conducted an FDE on BCS-F R3.2.4 at all U.S. ADSs in accordance with the DOT&E-approved Test and Evaluation Master Plan and FDE test plan in April 2017.
- Prior to initiating the FDE on BCS-F R3.2.4, the Air Force elected to defer fielding of the intrusion detection capabilities.
- In September 2017, the Air Force initiated test and evaluation of the replacement intrusion detection system and firewall capabilities. This testing is ongoing and will not be completed until FY18.

- In addition to the Radiant Mercury Guard and ongoing intrusion detection system and firewall capabilities upgrade, the BCS-F Program Office has begun collaboration meetings to plan for a future BCS-F system cybersecurity assessment.

Assessment

- During the April to June 2017 dedicated operational test events at the ADSs and RAOCs, the Air Force adequately tested BCS-F R3.2.4.
  - Most of the contents of BCS-F R3.2.4 demonstrated the required capabilities for the NORAD ADSs and RAOCs, as well as the USPACOM Hawaii RAOC to execute command and control and air battle management to support air sovereignty and air defense operations.
    - While BCS-F R3.2.4 resolved numerous previously known deficiencies in battle management and mission support operations, it resulted in several new deficiencies. The most significant of these deficiencies adversely affected the integration of FAA-sourced flight plans.
    - The Air Force is planning for regression testing of a planned system update to resolve this deficiency.
  - During developmental testing, a cybersecurity vulnerability inspection of BCS-F R3.2.4 revealed vulnerabilities that could pose risks to homeland air sovereignty and air defense mission.
  - Due to delays in the development of the WAS sensor, the Air Force did not complete systems integration and operational testing of WAS with BCS-F.
- Although the Air Force did not collect sufficient operational test data to demonstrate the system availability and reliability with statistical confidence, BCS-F R3.2.4 is maintainable and reliable.
  - During 773.43 hours of testing, BCS-F R3.2.4 demonstrated a 99.97 percent operational availability, experiencing 14 minutes of system downtime.
  - Operating with BCS-F R3.2.4, the ADSs and RAOCs demonstrated a Mean Time Between Corrective Maintenance Actions (MTBCMA) of 9.2 hours.
  - The overall MTBCMA did not meet the operational requirement of 100 hours MTBCMA. The MTBCMA for Critical Field Repair Actions (2 failures) was 386.6 hours and the MTBCMA for Non-Critical Field Repair Actions (84 failures) was 9.4 hours.
- BCS-F R3.2.4 technical documentation and training for the system remains deficient.
  - Due to poorly developed system maintenance documentation, numerous discrepancies in system documentation were discovered during the FDE at each ADS and RAOC.
  - ADS and RAOC leaders are concerned the training provided during initial delivery of new capability is not at an appropriate level of detail, and not resourced to support immediate transition to unit operations and maintenance personnel. This is significant when considering ADS and RAOC commanders are engaged in continuous 24/7 real-world mission operations and are not resourced for development of new equipment and new system capability training for all unit personnel.
- The system survivability against cyber threats remains unknown. Changes in the system architecture have been implemented since BCS-F R3.2.2. While the Air Force has conducted periodic cybersecurity vulnerability inspections during developmental testing, BCS-F has not had a comprehensive cybersecurity assessment since 2012.
- To assess BCS-F system reliability and availability with the BCS-F R3.2.4 upgrades, each ADS and RAOC conducted a 2 to 3 week operations trial period at the end of the FDE.
  - After completion of the operations trial period, during which no additional system discrepancies were identified, ACC and each ADS and RAOC transitioned to operational employment of the BCS-F system with the BCS-F R3.2.4 upgrade.
  - The assessed deficiencies identified during the FDE, including the FAA flight plan integration deficiency, have acceptable operator workarounds that effectively mitigated any negative effects on mission due to operational employment of the system.

Recommendations

- Status of Previous Recommendations. The Air Force still needs to:
  1. Provide training instruction and resources on new capabilities in a format that minimizes the impact on personnel scheduling and availability while conducting a 24/7 real-world mission.
  2. Ensure accurate documentation of system upgrades and new capabilities to minimize the number of deficiencies identified during fielding and OT&E.
  3. Develop a method to monitor BCS-F life-cycle system operational availability and reliability in order to inform program life-cycle management and sustainment policies.
  4. Complete a system cybersecurity assessment to identify, prioritize, and correct cybersecurity deficiencies.
- FY17 Recommendations. None.