Battle Control System – Fixed (BCS-F)

Executive Summary

- The Air Force completed a Force Development Evaluation (FDE) to evaluate operational effectiveness; interoperability; operational suitability; impact on tactics, techniques, and procedures; and cybersecurity postures on the Battle Control System – Fixed (BCS-F) Increment 3, Release 3.2.3 (R3.2.3) at all U.S. air defense sites in April 2016.
- BCS-F R3.2.3 is still not survivable against potential cyber-attacks despite the Air Force's efforts to resolve critical cybersecurity deficiencies.
- The BCS-F R3.2.3 has operational effectiveness deficiencies in system track management and datalink operations. The operators are able to use workarounds to mitigate these deficiencies to an acceptable level.
- The BCS-F R3.2.3 is operationally suitable with deficiencies in:
  - System maintenance documentation
  - Training program on system operations and maintenance
  - Lack of cybersecurity policies
  - Lack of program life cycle management policies and plan (i.e. Help Desk management, maintenance and repairs reporting, and spares management)
- All U.S. air defense sites were utilizing R3.2.3 in April 2016. Upon completion of the FDE, the Air Force formally fielded R3.2.3.

System

- BCS-F is the tactical air surveillance and battle management command and control system for the continental U.S. and Canadian air defense sectors (ADS)—Eastern ADS, Western ADS, Canadian ADS—of the North American Aerospace Defense Command (NORAD), the NORAD Alaska Regional Air Operations Center (RAOC), and U.S. Pacific Command's (PACOM) Hawaii RAOC.
- The system utilizes commercial off-the-shelf hardware within an open-architecture software configuration and operates within the NORAD and PACOM air defense architecture.
- The BCS-F R3.2.3 software upgrade includes the following system enhancements:
  - Increases maximum sensor and radar processing capacity, from 200 to 300 sensors
  - Fixes for 12 cybersecurity deficiencies previously identified
  - Updates to the air defense sector site radar parameters
  - Fixes for the operations display and the graphical user interface
  - Upgrades to the Internet Protocol converter/radar interface

- Also, the BCS-F R3.2.3 upgrade provided the following changes to system sustainment:
  - A software development/logistics support transition from contractor to government (520 Software Maintenance Squadron)
  - Updated Technical Order and System Manual documentation
  - Updated system training materials
- BCS-F R3.2.3 was designed to include the capability to interface with and process data from a sensor in the Wide Area Surveillance (WAS) program.
  - Due to WAS' lack of readiness, the Air Force did not conduct operational testing of WAS with BCS-F R3.2.3, but will evaluate sensor integration during operational testing of BCS-F R3.2.4.

Mission

- The Commander, NORAD and Commander, PACOM 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 PACOM 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 November 2015 through April 2016, the 605th Test and Evaluation Squadron conducted FDE on BCS-F R3.2.3 at all U.S. ADSs in accordance with a DOT&E-approved Test and Evaluation Master Plan and test plan.

- Upon completion of the FDE, the Air Force formally fielded R3.2.3. All U.S. ADSs were utilizing BCS-F R3.2.3 by April 2016.
- Canadian Air Defense Forces operationally accepted R3.2.3 in June 2016.

Assessment

- BCS-F R3.2.3 resolved 22 deficiencies in operational effectiveness and suitability associated with battle management and support operations.
  - These deficiencies were discovered during previous Increment 3.2 (R3.2, R3.2.0.1, R3.2.2) operational testing events.
  - Developmental testing and FDE of BCS-F R3.2.3 revealed 45 new deficiencies associated with battle management and support operations.
  - Operational testing of BCS-F R3.2.3 revealed two significant effectiveness deficiencies in system track management and two significant deficiencies in datalink operations.
  - Operator workarounds mitigated these deficiencies to an acceptable level.
- Although the Air Force did not collect sufficient operational test data to demonstrate the availability and reliability requirements with statistical confidence, BCS-F R3.2.3 is assessed as maintainable and reliable.
  - During 1,134.68 hours of testing, BCS-F R3.2.3 experienced 7 minutes of downtime in order to troubleshoot two system failures (a Category I and a Category II) at NORAD's Eastern ADS. This resulted in an operational availability of 99.99 percent (the 80 percent confidence interval is 99.79 to 99.99 percent).
  - Due to a lack of effective life-cycle management policies and plan, accurate data to assess overall system availability and reliability were not available.
  - BCS-F R3.2.3 was maintainable for routine maintenance actions, but the observed Mean Time Between Corrective Maintenance Action (MTBCMA) of 17 hours did not meet the requirement of 100 hours. This was not a critical shortfall since the maintenance actions had no negative effect on operations or operator workload.
  - After further analysis of maintenance activity, two types of maintenance actions were identified: Critical Field Repair and Non-Critical Field Repair.
  - A Critical Field Repair is assessed when a fault, failure, or malfunction results in the loss of any system's mission essential function as specified in the mission essential system list. Also, a critical failure includes greater than 10 percent of operator workstations becoming inoperative. A failure is not considered critical if mission operations are restored within 2 minutes.
  - MTBCMA for Critical Field Repair Actions (2 failures) was 211 hours and MTBCMA for Non-Critical Field Repair Actions (76 failures) was 17 hours.
  - In order to better understand system maintainability, future assessments may require separating Critical and Non-Critical MTBCMA measurements and identifying appropriate threshold requirements for each.
- While BCS-F R3.2.3 is operationally suitable, technical documentation and training for the system remains deficient. These deficiencies include:
  - System maintenance documentation
  - Training program on system operations and maintenance
  - Lack of cybersecurity policies
  - Lack of program life-cycle management policies and plan (i.e. Help Desk management, maintenance and repairs reporting, and spares management)
- Since only minor cybersecurity fixes were included in BCS-F R3.2.3, DOT&E assesses R3.2.3 remains deficient in all cybersecurity assessment areas. The system is poorly equipped to protect, detect, react, and restore/recover from attacks by current cyber threats, despite the fact that BCS-F R3.2.2 was designed to resolve many critical cybersecurity deficiencies. To address previously identified deficiencies, the Air Force implemented the Computer Network Defense Service Provider (CNDSP) agreement in 1QFY15. However, the Air Force has not conducted a cybersecurity assessment of BCS-F since the CNDSP was implemented.

Recommendations

- Status of Previous Recommendations. The Air Force satisfactorily addressed three of the previous recommendations. The Air Force still needs to:
  1. Correct and formalize all BCS-F Increment 3 system documentation and training deficiencies.
  2. Develop a plan for remote workstation management to include sustainment, training, documentation, and cybersecurity compliance.
  3. Upgrade the System Support Facility to support a more robust BCS-F developmental and operational testing capability in order to minimize the impact of overall testing at the operational air defense sector sites.
  4. Improve reliability to meet the threshold requirement for MTBCMA.
  5. Re-assess system cybersecurity vulnerabilities and correct identified cybersecurity deficiencies.
  6. Re-evaluate BCS-F survivability against cyber-attacks after the CNDSP has been implemented.
  7. Ensure appropriate policies, procedures, and tools exist for system administrators to effectively detect unauthorized intrusions.
- FY16 Recommendations. The Air Force should:
  1. Correct system operational effectiveness deficiencies.
  2. Correct and formalize all BCS-F R3.2.3 system operations and maintenance documentation, policy, and training deficiencies.
  3. Update the system threat assessment report for BCS-F.