Business Systems Modernization (BSM) – Energy

Executive Summary

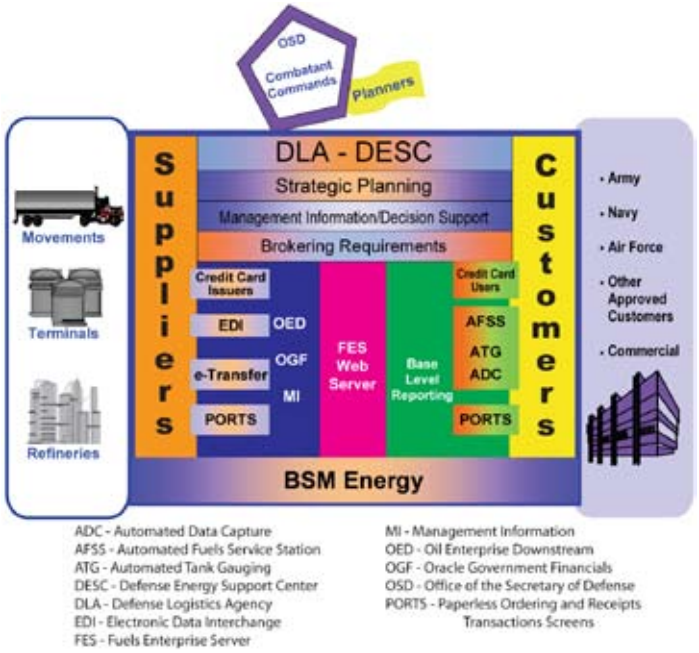
- The Joint Interoperability Test Command (JITC) completed an operational assessment of Business Systems Modernization (BSM)-Energy in August 2007.
- Test results showed that BSM-Energy was operationally effective but not operationally suitable, principally due to Information Assurance (IA) deficiencies.
- In conjunction with the operational assessment, the Defense Logistics Agency Computer Emergency Response Team (DLA CERT) completed a Red Team penetration test. Test results showed that IA deficiencies existed at both the Enterprise and Base Level systems.
- The Defense Logistics Agency (DLA) is developing a Plan of Actions and Milestones to address the IA issues identified by the DLA CERT and JITC.
- After the IA issues have been addressed, the DLA CERT and JITC will verify the correction of the deficiencies.

System

- BSM-Energy is an integrated database system using an open systems architecture design, which consists of two levels, the Base Level and the Enterprise Level.
- The Base Level system collects transaction data at the fuels distribution point, while the Enterprise Level processes ordering, supply, and financial functions.

Mission

The Defense Energy Support Center (DESC), the designated DLA agent in conducting DoD management of energy, uses



BSM-Energy to collect point-of-sale data, manage fuels inventory and war reserves, execute purchase orders, conduct financial and accounting management, and administer fuels distribution management.

Activity

- The JITC completed an operational assessment of BSM-Energy in August 2007 in accordance with the DOT&E-approved Test and Evaluation Master Plan and Operational Assessment Plan.
- In conjunction with the operational assessment, the DLA CERT completed a Red Team penetration test to determine the IA posture of BSM-Energy.

Assessment

- The operational assessment did not find any significant operational effectiveness concerns. DOT&E considered BSM-Energy operationally effective. However, test results showed that IA deficiencies requiring resolution existed at both the Enterprise and Base Level systems. DOT&E considered BSM-Energy not operationally suitable.
- The DLA CERT penetration test, corroborated by the JITC operational assessment findings, identified a number of IA vulnerabilities both at the Enterprise and Base Level systems that could be exploited to gain unauthorized access:
  - The authentication mechanism implemented was inadequate, which could allow unauthorized users to gain full control of the systems.
  - Training for both system administrators and users was lacking, specifically in the areas of intrusion detection and reaction.
  - There were no periodic perimeter defense checks of the system firewalls to ensure adequate IA protection.
  - The IA Concept of Operations for the system was deficient.

Recommendations

- Status of Previous Recommendations. There were no previous recommendations for BSM-Energy.
- FY07 Recommendations.

1. DLA should finalize and execute a Plan of Actions and Milestones to address IA issues identified by the DLA CERT and JITC. Major remediation actions required include:
   - DLA must mitigate or eliminate vulnerabilities caused by inadequate authentication (e.g., passwords, Public Key Infrastructure certificates) that could allow unauthorized users to gain full control of the systems.
   - Training should be improved to enable system administrators to more effectively detect and react to attempts at unauthorized entry.
   - System administrators should perform periodic perimeter defense checks of the system firewalls to ensure adequate IA protection.
   - The program manager should develop a more comprehensive IA Concept of Operations that addresses major IA functions of protection, detection, reaction, and restoration for BSM-Energy. Additionally, intrusion response training and drills should be conducted periodically to improve incident reporting procedures and intrusion responses.
2. After the IA issues have been addressed, the DLA CERT and JITC should verify the correction of the deficiencies.