

## **Enterprise Cyber Security Program – ECSP (EA-52)**

### *Authoritative Source*

- VA IT Portfolio BY-2008

### *Stakeholders*

- All veterans, their dependents, and their survivors
- VA Administrations
- VA Business Partner Agencies
- VA Managers and Employees

### *Related Segment Architectures*

- “Proposed” Information Management Services Segment
- Identity Management Services Segment

### *Mission and Organization*

The Enterprise Cyber Security Program (ECSP) establishes and maintains enterprise-wide security controls and measures. ECSP formulates, implements, and oversees the Department’s enterprise-wide security program. ECSP also provides a continuous cycle of risk assessment, security policy and procedure improvement and subsequent testing of improved security controls. ECSP is comprised of two management components (ECSBAP and Field Ops) and two technical components (CIPP and SCMS).

The Enterprise Cyber Security Business Assurance Program (ECSBAP):

- Establishes VA IT security policies and procedures;
- Oversees the Department-wide Risk Management and Certification and Accreditation (C&A) program;
- Coordinates VA’s FISMA Reporting and Compliance Programs;
- Updates the Department IT Security Program Plan; and
- Provides procurement, budgeting, personnel, and capital planning support for the cyber security investment.

Field Operations and Information Security Officer Support Service (Field Ops):

- Provides oversight for the facility based Information Security Officers (ISOs);
- Sponsors the Department’s security awareness training;
- Produces VA’s role-based training for ISOs;
- Organizes VA’s Annual Information Security Conference.

In FY 2008, because of the VA IT Reorganization Plan, ECSP will assume the responsibility for the Information Security Officer staff.

ECSP’s three technical components manage the implementation of enterprise-wide activities that are approved by the Chief Information Officer (CIO) as common security controls and

initiatives, and are derived through the combined results of program risk assessments, FISMA Self-Assessment Surveys, the CIO/Program Official Annual Review, and consultation with the VA Office of Inspector General:

- The Critical Infrastructure Protection Program (CIPP) directs the operation of Security Operations Center (SOC), which is responsible for providing a centralized incident response and recovery mechanism, as well as other global security services such as penetration testing, vulnerability scanning, firewall management, intrusion detection monitoring, event correlation, and associated audit log analysis.
- The Security Configuration Management Service (SCMS) oversees patch management and the anti-virus program; and deploy host-based intrusion prevention, anti-spyware, and anti-spam solutions.

### *Concept of Operations*

IT Security is addressed both at the enterprise and project levels, with funding provided by VA's Administrations, which receive direct appropriations. At the enterprise level, ECSP, which is managed by the Office of Cyber and Information Security (OCIS), represents those activities that provide a continuous cycle of risk assessment, modification of policies and procedures to reflect changes in the risk environment, identification of mitigating security controls and the on-going testing of those controls to ensure their effectiveness. It also provides oversight for a segment of Information.

- Anti-Virus Program: The VA anti-virus program is deployed across approximately 150,000 desktops and servers, representing one of the largest virus protection programs in the world. Its implementation is based, in part, on the findings of the 2004 Computer Crime and Security Survey, This annual survey is conducted by the Federal Bureau of Investigation/Computer Security Institute; its 2004 findings indicated that productivity losses associated with virus and worm incursions represented the single largest category of industry/government IT-related losses, and that 99% of all survey respondents reported implementing anti-virus protections as a mitigating security control. Insurance industry estimates indicate that approximately \$17 billion dollars in losses are experienced each year based on emerging virus and work attacks. These estimates include a general cost-benefit valuation for virus protection indicating that, for each dollar spent, an organization avoids \$11 in lost productivity that would have occurred through successful virus attacks.
- Authentication-Authorization Program: During Congressional testimony in 2005, VA leadership advised that AAIP, which is the integration of commercial-off-the-shelf identity and access management technology to allow users to access VA computers through a smart card token, demonstrated the capability to recover up to 45 minutes per day of individual clinician time through simplified log on processes in a thin-client environment. Industry statistics from the Gartner Group estimates an 18-month return on investment for such technologies, indicating that VA could achieve up to several million dollars of monthly cost savings monthly related to the use of AAIP for logical and physical access control after initial investment costs are recouped.
- Security Configuration Management Services: The Department's Security and Configuration Management Service (SCMS) was evaluated by the Gartner Group, with

several SCMS methodologies subsequently being referenced as best practices and viable strategies to mitigate worms and viruses, as indicated in the Gartner Group Research Paper ID Number AV-22-2700, Strategies to Combat Rapidly Spread Cyber-attacks.

### ***EA Investment Scoring***

The following table provides the EA evaluation score for BY-2008 (this is the project's most recent Exhibit-300 budget request). Scores are provided for business, data and implementation issues and for an overall project average. The Exhibit-300 EA evaluation procedure is defined within the Enterprise Architecture Portal "Procedures Tab"; all scoring is based on a scale from 0 through 5.

VA EA Evaluation			
Business	Data	Implementation	Average
3.33	2.00	3.20	<b>2.80</b>

### ***Project Value Proposition, Performance Measures and Measured Results***

The following table identifies the VA and PMA business objectives that this project will satisfy, along with the performance metrics with which project success will be evaluated. For projects that are mature enough to have produced measured results, those results are also provided.

Project Value Proposition			
Support for PMA Initiatives 1.A.13.a & 1.A.13.b	Support for VA Strategic Goals 1.A.29	Project Metrics 1.D.1	Project Results/Outcomes 1.D.1
<p><b>Expanded E-Government</b> ----ECSP supports the goal of Expanded E-Government through its PKI implementation effort which will ensure that</p> <p>(1) electronic transactions with and within government are private and secure; and</p> <p>(2) by decreasing the amount of IT misuse, fraud, and the potential for unauthorized disclosure of veteran and sensitive data, while ensuring non-repudiation of transactions.</p>	<p><b>One VA</b> This objective is addressed through deploying a Department-wide suite of IT controls (firewalls, intrusion detection systems, vulnerability scanning, penetration testing), certify and accredit VA IT systems and major applications to ensure compliance with NIST guidance and standards; provide security awareness training for all personnel, and role-based training for VA personnel with significant security responsibilities; and, oversight of configuration management practices.</p> <p><b>Quality of Life</b> The Enterprise Cyber Security Program acts to protect VA IT systems from internal and external attack, as well as other interruptions and/or service degradations. It provides an infrastructure that will allow veterans to securely conduct business with VA electronically, as well as access or update personal information with assurance that the information will be kept confidential, and that transactions will be processed accurately and in a timely manner.</p>	<p><b>Measurement-1 Indicator</b> Complete C&amp;A activities for all operational systems, on a 3-year recurring cycle (2005-Baseline =90% Certified); (2006-Target= Complete C&amp;A on remaining 10%).</p> <p><b>Measurement-2 Indicator</b> Establish Department wide minimum mandatory security configurations standards for each operating system (2005 baseline =2 of 8 Operating Systems or 25%). (2006 target = 4 of 8 Operating Systems or 50%)</p> <p><b>Measurement-3 Indicator</b> Increase the number of Information Security Officers (ISO) trained in the use of risk assessment tools and procedure (2005 baseline =27) (2006 target = 52 or an additional 25 ISOs).</p> <p><b>Measurement-4 Indicator</b> In 2006, Field an automated</p>	<p><b>Measurement-1 Results</b> Results will be measured by Q3-FY2007</p> <p><b>Measurement-2 Results</b> Results will be measured by Q3-FY2007</p> <p><b>Measurement-3 Results</b> Results will be measured by Q3-FY2007</p> <p><b>Measurement-4 Results</b> Results will be measured by Q3-FY2007</p>

Project Value Proposition			
Support for PMA Initiatives 1.A.13.a & 1.A.13.b	Support for VA Strategic Goals 1.A.29	Project Metrics 1.D.1	Project Results/Outcomes 1.D.1
		tool to conduct an annual security assessment of every Department system and program. (2005- baseline 100% systems surveyed but automated-tool not developed) (2006-Target = continue to survey 100% of systems and develop automated tool).	

***Enterprise Impact***

This investment produces a consistent, enterprise-wide solution to meeting security requirements; repeatable practices are developed and followed and compliance is centrally measured and reported. Policy guidance, training, and certification are also developed and managed at an enterprise level, to support security activities that are managed at the project or local facility level.

***Project Status***

Funded through BY-2007 (O&M)

Project Operational