Federal Agency Security Practices (FASP)
Federal Information Security Management Act (FISMA) Reporting Project
Submitted by:
Department of Veterans Affairs'
Office of Cyber and Information Security (OCIS)

Background

"*For those who have borne the battle, for their widows, and their orphans*". In 1865, Abraham Lincoln expressed this founding idea, which has become the guiding principle of the Department of Veterans Affairs. Toward that end, VA has become the nation's largest health care and cemetery services provider and the provider and guarantor of significant other financial benefits and services for 25.5 million living veterans. With 225,000 employees managing services and benefits of over $60 billion annually, its information infrastructure connects with veterans and partners nationwide and represents an important piece of the nation's critical infrastructure.

The VA Office of Information and Technology (OI&T) is a critical enabling component for this important responsibility. The mission of the Office of Cyber and Information Security (OCIS) within OI&T is two-fold:

- To provide information security services to veterans and their beneficiaries that protect their private information and enable the timely, uninterrupted and trusted nature of those services, and

- To provide assurances that cost-effective information security controls are in place to protect automated information systems from financial fraud, waste and abuse.

To oversee the confidentiality, integrity, availability and accountability for use of the health and benefit information processed on its information systems, VA needs dedicated, highly skilled professionals to oversee and appropriately report on the cyber security of its networks. This Federal Agency Security Practices (FASP) write-up sets out the process used by OCIS to improve reporting on VA compliance with the Federal Information Security Management Act of 2002 (FISMA).

Problem

Management of cyber security for VA's extensive and geographically distributed information assets is complicated by the fact that the systems and information technology staff supporting individual VA lines of business are not yet fully integrated under a standard architecture or organizational structure. The historical problems of decentralized architecture and cyber security management have complicated the process of recording and reporting results of actions required by FISMA and other Federal regulatory requirements.

Among the major challenges facing VA's FISMA compliance program are:

- Department-wide FISMA reporting, including oversight of the implementation of FISMA requirements,
- Department-wide FISMA compliance assessment, and
- Department-wide FISMA Annual Reports and quarterly Plans of Action and Milestones (POA&M) documents for OMB.

Solution

With the endorsement of VA's Secretary and Chief Information Officer (CIO), OCIS brings FISMA management under its management purview, coordinating issues of compliance with VA's diverse IT and business communities and simplifying logistic control. OCIS oversees the implementation of VA's FISMA program, addressing the challenges presented for compliance. Given similarities in compliance requirements, OCIS includes the entire realm of security remediation in this program; including requirements of VA Office of Inspector General (OIG), General Accounting Office (GAO), the Congress, and other oversight and compliance organizations. This project also conducts reviews of VA Capital Plans (Exhibits 300) to ensure that program managers have adequately linked security requirements to FISMA POA&M deficiencies that are targeted for remediation, and have adequately specified sufficient resources to secure their information technology projects. By placing this Project in the same organization also responsible for oversight of security controls, VA's OCIS has simplified remediation efforts.

Process

OCIS provides the funding, management staff, and authority to manage the Department's FISMA Reporting Project. A FISMA Reporting Project Charter identifies the management structures to ensure that changes and issues affecting project completion are properly controlled. A Project Control Board (PCB) consists of a Project Manager and supporting functional team leaders. An Executive Steering Committee (ESC) furnishes executive direction to the PCB.

Major Milestones, Activities, and Goals

- Oversee completion of all requirements associated with FISMA.
- Provide compliance subject matter experts to VA's IT and business line customers.
- Implement a FISMA database including management, user and system documentation, user assistance, training, data collection, and compliance reporting.
- Review of VA capital plans to ensure adequate security resources are requested to address FISMA deficiencies.

- Report on the status of FISMA-related activities to the Federal oversight community, including:
    - Quarterly POA&M Reporting Cycle
    - Annual FISMA Report to OMB
    - Annual status report for submission with VA's budget
- Achieve Federal Information Technology Security Assessment Framework (FITSAF) Level 4.

Contacts

Bruce A. Brody, CISM, CISSP
Associate Deputy Assistant Secretary for Cyber and Information Security
Department of Veterans Affairs
202-273-8007
bruce.brody@mail.va.gov

Pedro Cadenas, Jr.
Deputy ADAS for Cyber and Information Security
Department of Veterans Affairs
202-273-8431
pedro.cadenas@mail.va.gov

Michael S. Arant, CISSP
Cyber Security Liaison
Department of Veterans Affairs
michael.arant@mail.va.gov