Federal Agency Security Practices (FASP)
Cyber Security Practitioner Professionalization (CSPP)
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 the cyber security of its networks. This Federal Agency Security Practices (FASP) write-up sets out the process used by OCIS to upgrade the cyber security skills of existing VA staff incorporating common, measurable standards.

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 became the principal causal factors for the Material Weakness finding regarding the Department's information security technology controls under the Federal Managers Financial Integrity Act (FMFIA). Despite their dedication, the geographically distributed cyber security staff was challenged and frustrated by disparate levels of expertise and sometimes conflicting guidance. Measurably improving their cyber security knowledge and capabilities within a common set of expectations is crucial to remedy the VA Material Weakness and enhance the Department's ability to make the progress required by OMB and the Federal Information Security Management Act (FISMA).

Solution

In response to the issues of instructing, motivating, empowering, and retaining cyber security staff, OCIS established the VA Cyber Security Practitioner Program (CSPP). The objectives of CSPP are to:

- Establish a package of Department-wide training to ensure diverse staff elements receive quality, relevant, and standard training experiences;
- Ensure that staff are tested, certified, and *qualified* to act locally in the interest of VA-wide cyber and information security;
- Maintain, improve, and advance security training as VA and its IT program react to the dynamics of the risk environment;
- Provide empowerment in the form of a credential to demonstrate staff are *authorized* to act locally in the interest of VA-wide cyber and information security;
- Institute a career progression in cyber security to provide mobility and opportunity; and
- Provide incentives to motivate trained, certified, and empowered staff to remain in the VA cyber and information security career field.

The CSPP is comprised of the following primary program elements.

- A "Body of Knowledge" (BOK) reflecting the specific needs of cyber and information security in VA and government.
- Twenty-four hours of classroom training based on the BOK delivered at four distributed venues.
- Twelve hours of VA Intranet web-based training and on-line test, also based on the BOK.
- An annual Department conference, VA InfoSec, which provides another 24 hours of training plus information about VA's cyber security programs and services.
- Standard Position Descriptions (PD) and Performance Standards (PS) defining a career progression.
- A credential symbolizing an individual's empowerment.
- A program of monetary and non-monetary incentives.

Process

OCIS provides the funding, management staff, and authority for the CSPP to manage all components of this program. A CSPP Charter identifies the management structures to ensure 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

- Develop Body of Knowledge
- Deliver Classroom Training
- Stage VA InfoSec Conference
- Implement On-Line Training and Testing
- Issue Certifications to those who achieve passing scores
- Develop Standard PDs and PSs
- Issue Credentials
- Implement Incentives

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