Federal Agency Security Practices (FASP)
Enterprise Cyber Security Infrastructure Project (ECSIP)
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, it is essential to use multiple layers of coordinated information and cyber security protective tools and to monitor those tools in real-time. The challenge is to develop and install an *effective* suite of tools that maximize *efficiency* for the network and the monitoring process while maximizing *economies* of scale available in very large enterprises.

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 within the Department created a series of patchwork security architectures, sometimes-incompatible products, and uneven mitigation of risks.

Because of the lack of effectiveness of this patchwork security infrastructure, VA had become the primary propagator of viruses within the Federal government. The cost of network operations had soared with over 200 uncertified and unevenly protected independent Internet gateways. The result was an inefficient, technically and organizationally diverse information enterprise that was unacceptably vulnerable to compromise and disruption because of disjointed and uncoordinated implementation of technical cyber security controls.

Solution

In response to the issue of disjointed and uncoordinated implementation of technical cyber security controls, VA's OCIS established the Enterprise Cyber Security Infrastructure Project (ECSIP), a strategic initiative cutting across the VA enterprise. The goal of ECSIP is to protect VA's information technology assets nationwide by establishing and maintaining a secure VA-wide IT security framework upon which VA business processes can reliably deliver robust services to veterans.

VA has adopted a "defense-in-depth" approach to defend its enterprise comprised of seven points of cyber security doctrine[1] established by VA IT executives. ECSIP directly addresses five of the seven points:

- Protect Network Infrastructure Services
- Boundary Protections
- Intrusion Detection Systems and Services
- Online Virus Protection
- Active Security Monitoring

The ECSIP program is comprised of the following primary program elements.

- A project that secures the VA network boundary with premier firewall, network monitoring, and intrusion detection technologies. This project migrates services from over 200 independent gateways down to 4 national gateways and potentially others to establish a controllable number of entry and exit points to the VA network.
- A project to equip, manage, and staff two Network and Security Operations Centers to monitor VA devices at the corporate communications carrier facilities, operating 24x365.
- A project to provide vulnerability assessment and penetration testing tools, and infrastructure to support periodic network scanning.
- A project to provide infrastructure, maintenance, and certification of anti-virus software, real-time virus reporting and alerting capability, and anti-virus training to optimize use of available tools.

Process

OCIS provides the funding, management staff, and authority for ECSIP to manage all components of this program. An ECSIP 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

[1] Protect Network Infrastructure Services, Protect the Boundary, Implement Intrusion Detection Systems and Services, Implement Online Virus Protection, Actively Monitor Security Status, Secure Department Operating Systems, and Secure Protocols.

leaders. An Executive Steering Committee (ESC) furnishes executive direction to the PCB.

Major Milestones

- Develop ECSIP Implementation Plan and Schedule for All Sites
- Implement ECSIP "Defense-in-Depth" at All Sites
- Integrate Enterprise-Wide Advanced Technology Solutions
- Operate and Support National Gateways/Retire Uncontrolled Gateways
- Maintain Department-Wide Anti-Virus Program
- Establish Advanced Technology Testing and Acquisition

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