VA Office of Inspector General

Office of Audits and Evaluations

“CIO/IG Interface with Department of Veterans Affairs”

Federal Computer Security Managers’ Forum “Offsite” Meeting

May 15, 2018

Background

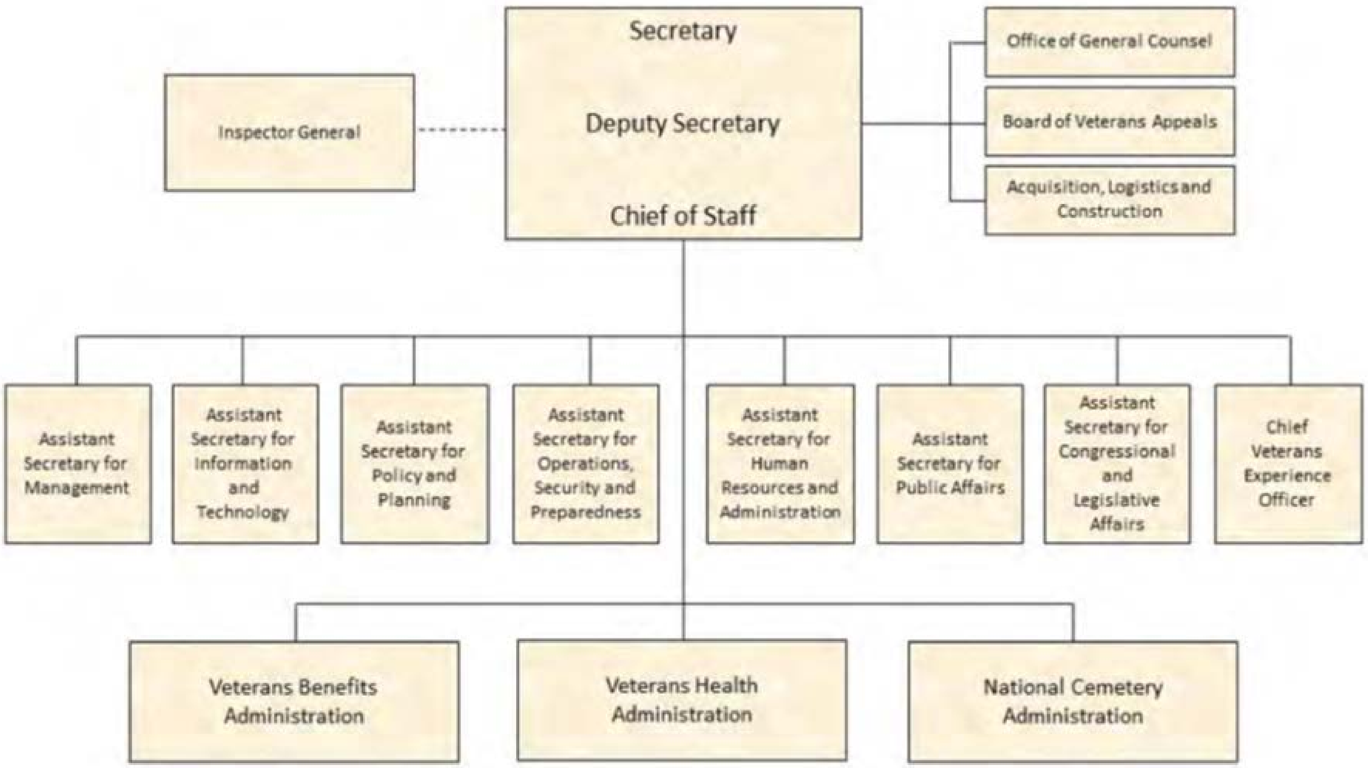
- Presenter: Michael Bowman – Director Information Technology & Security Audits Division; VA Office of Inspector General

- Theme: Standard practices the OIG utilizes to coordinate and conduct the annual audit of VA’s Information Security Program in accordance with FISMA.

VA OIG’s Current Role

- Assessing agency’s information security programs in accordance with FISMA
- Evaluating IT general and business process application controls
- Performing vulnerability and security configuration testing.
- Follow-up on prior year findings.
- Reporting results in accordance OMB’s annual FISMA reporting instructions.

Department of Veterans Affairs Organizational Structure



Secretary

Deputy Secretary

Chief of Staff

Inspector General

Office of General Counsel

Board of Veterans Appeals

Acquisition, Logistics and Construction

Assistant Secretary for Management

Assistant Secretary for Information and Technology

Assistant Secretary for Policy and Planning

Assistant Secretary for Operations, Security and Preparedness

Assistant Secretary for Human Resources and Administration

Assistant Secretary for Public Affairs

Assistant Secretary for Congressional and Legislative Affairs

Chief Veterans Experience Officer

Veterans Benefits Administration

Veterans Health Administration

National Cemetery Administration

Department of Veterans Affairs Organizational Structure

- FY 2018 Budget = $ 186 billion
- FY 2019 Budget = $ 198 billion
- FY 2018 Full Time Equivalents = 350k personnel
- Program Offices – Lines of Business
  - **Veterans Health Administration:** 1700 sites of care for 23 million veterans. 23 VISNS support geographical areas throughout US.
  - **Veterans Benefits Administration:** 56 Regional Offices that administer compensation, pension, education, and loan programs
  - **National Cemetery Administration:** 135 national cemeteries. Manages State cemetery grant program.

Department of Veterans Affairs Significant Systems

- Veterans Health Administration
  - **VistA:** Electronic Health Record system comprised of over 100 separate applications that support medical, financial, and acquisition functions.
  - **Computerized Patient Record System:** Supports the entering, reviewing, and continuously updating of patient information.
- Veterans Benefit Administration
  - **Veterans Benefit Management System:** Provides a paperless environment for veterans claims processing and benefits delivery.
  - **Benefits Delivery Network:** Mainframe system that processed benefits for Compensation, Pension, Education, and Employment Services.
  - **Veterans Service Network:** Suite of applications that provide benefit payment and accounting functionality.
- National Cemetery Administration
  - **Burial Operations Support System:** Contains the records of the interments at National, State Veterans', Post-Military, Department of Army, and Department of Interior cemeteries.

Office of Information & Technology Resources

- FY 2018 Budget = $4.056 billion
- Full Time Equivalents = 7,387
- Program Offices:
  - Information Technology Operations and Services: FTEs = 5,391
  - Enterprise Program Management Office: FTEs = 1,081
  - Office of Information Security: FTEs = 522
  - Office of Quality, Privacy, and Risk: FTEs = 194
  - Information Technology Resource Management: FTEs = 90
  - Architecture, Strategy, and Design: FTEs = 78
  - Account Management Office: FTEs = 22
  - Interagency Program Office: FTEs = 9

Office of Information & Technology Information Security Responsibilities

- VA has approximately 240 systems identified as General Support Systems or Major Applications.

- VA has 5 centralized major data centers that maintain financial management systems; process compensation, pension, and other veteran benefit payments; and manage the veteran life insurance programs.

- VA's has many legacy systems have been obsolete for years. Systems are costly to maintain, cumbersome to operate, and difficult to secure.

- De-centralized system architecture makes the enforcement of an agency-wide information security program very difficult.

FISMA Overview

- Annual FISMA audit is high profile in nature.
- VA OIG meets annually with the VA Secretary to discuss the results of our FISMA audit.
- VA OIG has participated in several Congressional hearings to discuss the results of our past FISMA audits.
- VA Leadership has an organization priority to remove the IT Material Weakness.
- VA OIG leverages the annual FISMA audit to evaluate numerous information security controls each year.

Standard Practices for Conducting annual FISMA audits - Methodology

- Rules of Engagement to define technical audit tools, on-boarding practices, logistical requirements, and trusted agents.

- Comprehensive controls testing at 24 facilities each year to include all major data centers, VA Medical Centers, and VA Regional Offices.
  - Approximately 20% of mission critical systems tested each year.

- Technical tools include: NMAP, Nessus, AppDetective, WebInspect, Wireshark, and Kali-Linux.

- Consistent testing of mission critical systems and network devices general, application, and technical controls

Standard Practices for Conducting annual FISMA audits - Communication

- Conduct January meetings prior to launching the annual FISMA audit in March each year.
  - Changes in business practices are discussed early
  - Changes in security roles and responsibilities are discussed early
  - Completed corrective actions are discussed early

- Conduct Friday calls with OI&T to resolve logistical issues during the audit season.

- Present preliminary findings at the 24 site visits for vetting.
  - Present 24 draft site reports during the audit season for vetting.

Standard Practices for Conducting annual FISMA audits – Audit Focus

- We test a significant number of general, application, and technical controls each year.

- When evaluating the significance of security issues, we tend to focus on the following:
  - Weak passwords
  - Lack of access monitoring
  - Weak system configurations
  - Missing system security patches
  - Excessive system permissions
  - Unsupported computer platforms
  - Inconsistent security practices

- We evaluate these types of security issues each year when determining whether to downgrade the IT Material Weakness.

Standard Practices for Conducting annual FISMA audits – Reporting

- Conduct Exit Conferences at 24 VA facilities to discuss preliminary findings.
- Provide 24 Draft site reports to management for review.
- Provide the FISMA Cybersecurity Report for management's review.
- Provide the FISMA narrative report for management's review.
- Provide IT Management Letters for management's review.
- Provide the Financial Audit – Internal Controls Report for management's review.

Recent Improvements

- Implementation of Two-Factor authentication across the enterprise.

- Implementation of the Enterprise Cybersecurity Strategic Plan to address the IT Material Weakness.

- Collection of audit logs in support of an enterprise level security information and event management capability.

- Oversight of VA's Assessment and Authorization process.

Questions