GAO
Accountability • Integrity • Reliability
Highlights

Highlights from GAO-11-663T, a testimony before the Subcommittee on Oversight and Investigations, Committee on Veterans' Affairs, U.S. House of Representatives

May 11, 2011

INFORMATION TECHNOLOGY

Department of Veterans Affairs Faces Ongoing Management Challenges

Why GAO Did This Study

The use of information technology (IT) is crucial to helping the Department of Veterans Affairs (VA) effectively serve the nation's veterans, and the department has expended billions of dollars annually over the last several years to manage and secure its information systems and assets. VA has, however, experienced challenges in managing its IT. GAO has previously highlighted VA's weaknesses in managing and securing its information systems and assets.

GAO was asked to testify on its past work on VA's weaknesses in managing its IT resources, specifically in the areas of systems development, information security, and collaboration with the Department of Defense (DOD) on efforts to meet common health system needs.

What GAO Recommends

In previous reports in recent years, GAO has made numerous recommendations to VA aimed at improving the department's IT management capabilities. These recommendations were focused on: improving two projects to develop and implement new systems, strengthening information security practices and ensuring that security issues are adequately addressed, and overcoming barriers VA faces in collaborating with DOD to jointly address the departments' common health care business needs.

View GAO-11-663T or key components.
For more information, contact Joel C Willemssen at (202) 512-6253 or willemssenj@gao.gov or Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov.

What GAO Found

Recently, GAO reported on two VA systems development projects that have yielded mixed results. For its outpatient appointment scheduling project, VA spent an estimated $127 million over 9 years and was unable to implement any of the planned capabilities. The application software project was hindered by weaknesses in several key management disciplines, including acquisition planning, requirements analysis, testing, progress reporting, risk management, and oversight. For its Post 9/11 GI Bill educational benefits system, VA used a new incremental software development approach and deployed the first two of four releases of its long-term system solution by its planned dates, thereby providing regional processing offices with key automated capabilities to prepare original and amended benefits claims. However, VA had areas for improvement, including establishing business priorities, testing the new systems, and providing oversight.

Effective information security controls are essential to securing the information systems and information on which VA depends to carry out its mission. For over a decade, VA has faced long-standing information security weaknesses as identified by GAO, VA's Office of the Inspector General, VA's independent auditor, and the department itself. The department continues to face challenges in maintaining its information security controls over its systems and in fully implementing the information security program required under the Federal Information Security Management Act of 2002. These weaknesses have left VA vulnerable to disruptions in critical operations, theft, fraud, and inappropriate disclosure of sensitive information.

VA and DOD operate two of the nation's largest health care systems, providing health care to 6 million veterans and 9.6 million active duty service members at estimated annual costs of about $48 billion and $49 billion, respectively. To provide this care, both departments rely on electronic health record systems to create, maintain, and manage patient health information. GAO reported earlier this year that VA faced barriers in establishing shared electronic health record capabilities with DOD in three key IT management areas—strategic planning, enterprise architecture (i.e., a description of business processes and supporting technologies), and IT investment management. Specifically, the departments were unable to articulate explicit plans, goals, and time frames for jointly addressing the health IT requirements common to both departments' electronic health record systems. Additionally, although VA and DOD took steps toward developing and maintaining artifacts related to a joint health architecture, the architecture was not sufficiently mature to guide the departments' joint health IT modernization efforts. Lastly, VA and DOD did not have a joint process for selecting IT investments based on criteria that consider cost, benefit, schedule, and risk elements, which would help to ensure that the chosen solution both meets the departments' common health IT needs and provides better value and benefits to the government as a whole. Subsequent to our report, the Secretaries of Veterans Affairs and Defense agreed to pursue integrated electronic health record capabilities.