United States Government Accountability Office

GAO

Report to Congressional Committees

November 2010

HEALTH INFORMATION TECHNOLOGY

DOD Needs to Provide More Information on Risks to Improve Its Program Management

GAO-11-148

November 2010

HEALTH INFORMATION TECHNOLOGY

DOD Needs to Provide More Information on Risks to Improve Its Program Management

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-11-148, a report to congressional committees

Why GAO Did This Study

The National Defense Authorization Act for Fiscal Year 2010 directed the Department of Defense (DOD) to submit a report to congressional defense committees on improvements to the governance and execution of its health information management and information technology (IT) programs to support medical care within the military health system. DOD submitted its report to the appropriate House and Senate committees in June 2010. The act also directed GAO to assess the report and DOD's plan of action to achieve its goals and mitigate risks in the management and execution of health information management and IT programs. Specifically, GAO's objective was to determine whether DOD addressed the reporting requirements specified in the defense authorization act. To do this, GAO reviewed the report submitted by DOD, and analyzed it against the reporting requirements, prior GAO work examining DOD's health IT issues, DOD guidance, and industry best practices.

What GAO Recommends

GAO is recommending that DOD report additional details to address shortcomings in 4 requirements, including risk identification and assessment, risk mitigation planning, and corrective action planning. In comments on a draft of this report, DOD concurred with GAO's recommendation and described actions it is taking to address it.

View GAO-11-148 or key components. For more information, contact Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov

What GAO Found

DOD addressed 6 of the 10 reporting requirements included in the National Defense Authorization Act for Fiscal Year 2010 (see table). For example, it reported on its capability to meet the requirements for joint interoperability—the ability to exchange electronic patient health data—with the Department of Veterans Affairs. The department also reported on its capability to carry out necessary governance, management, and development functions of health information management and IT systems.

The department partially addressed the remaining 4 requirements, which pertained to identifying, assessing, and mitigating risks, as well as reporting on estimated resources required to optimally support health care IT and planning corrective actions to remedy shortfalls that DOD identified. For example, the department had identified and assessed risks, but the report did not fully disclose these risks or the meaning of the department's assessment. Also, the report did not fully identify the staff and funds needed, nor did it fully identify the organizations responsible and accountable for accomplishing risk mitigation activities. If not corrected, incomplete reporting to address these requirements could impede congressional oversight of the department's planned improvements.

GAO Assessment of DOD Compliance with Reporting Requirements

Requirement	GAO assessment
Assess the capability of the department's enterprise architecture to achieve optimal clinical practices and health care outcomes.	Addressed
Identify and assess risks associated with achieving timelines and goals of each health information management and technology program.	Partially addressed
Provide a plan of action to mitigate identified risks.	Partially addressed
Assess the appropriateness of the health information management and IT technical architecture and whether it leverages industry best practices.	Addressed
Determine DOD's capability for meeting requirements for joint interoperability with the Department of Veterans Affairs and progress made on establishing a joint virtual lifetime electronic record for members of the armed forces.	Addressed
Develop a corrective action plan to remedy shortfalls identified as a result of assessments.	Partially addressed
Estimate resources required in future years to achieve optimal IT support for health care clinical practices and compliance with applicable requirements.	Partially addressed
Analyze methods for procuring health information management and IT goods and services and the appropriateness of the application of legal and acquisition authorities.	Addressed
Analyze the department's capabilities for carrying out necessary governance, management, and development functions of health information management and IT systems.	Addressed
Recommend whether DOD health information and IT systems should be subject to requirements of defense business systems.	Addressed

Source: GAO analysis of DOD data.

Contents

Abbreviations

DOD	Department of Defense
EA	enterprise architecture
EHR	Electronic Health Record
IT	information technology
VA	Department of Veterans Affairs
VLER	Virtual Lifetime Electronic Record

GAO
Accountability * Integrity * Reliability

United States Government Accountability Office
Washington, DC 20548

November 17, 2010

Congressional Committees

The Department of Defense (DOD) plans to improve the quality of health care provided to service members and their beneficiaries by modernizing its health information systems and improving its sharing of electronic health information. This is to be carried out through a strategy that includes initiatives to modernize current electronic health record capabilities, improve the exchange of electronic health information with the Department of Veterans Affairs (VA), and support electronic medical data capture and exchange among private health care providers and state, local, and other federal agencies.

The National Defense Authorization Act for Fiscal Year 2010[1] required the Deputy Secretary of Defense to submit a report to Congress on the improvements that DOD is making to the governance and execution of health information management and information technology programs planned and programmed to electronically support clinical medical care within the military health care system.[2] The act specified 10 reporting requirements related to the governance and management of these programs. In accordance with the act, DOD developed its report, entitled *Improvements to the Governance and Execution of Health Information Management and Information Technology Programs.* DOD submitted the report to the Senate and House Armed Services Committees and Senate and House Appropriations Committees on June 23, 2010.

The act required GAO to assess DOD's report and plan of action to achieve the department's goals and mitigate risks in the management and execution of health information management and Information Technology programs. GAO was to assess the report no later than 30 days after it was submitted and provide our results to the congressional defense committees. Our objective was to determine whether DOD addressed the reporting requirements specified in the act.

[1]Pub. L. No. 111-84, § 716 (2009).

[2] The Military Health Care System employs 135,000 personnel in approximately 700 Army, Navy, and Air Force medical facilities in 12 domestic regions as well as European, Pacific, and Latin American regions.

To accomplish the objective, we reviewed the reporting requirements in the act, analyzed DOD's report prepared in response to the act, and reviewed related guidance, such as DOD's risk management and Software Engineering Institute guidance.[3] We then determined whether the reporting requirements were addressed or partially addressed. [4] We discussed our determinations with DOD's Office of the Deputy Chief Management Officer.

On July 23, 2010, we provided briefing slides to your staffs on the results of our study. The purpose of this report is to provide the published briefing slides to you and to officially transmit our recommendation to the Secretary of Defense. The briefing slides, including details on our scope and methodology, are reprinted in appendix I.

We conducted our work in support of this performance audit from June 2010 to November 2010, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

In summary, our study highlighted the following:

- DOD addressed 6 of the 10 reporting requirements included in section 716 of the fiscal year 2010 National Defense Authorization Act. For example, the department addressed the requirements to report on its assessment of the capability of the department's enterprise architecture to achieve optimal clinical practices and health care outcomes, its capability to meet requirements for joint interoperability with VA, and its methods for procuring health information management and technology goods. Also, the department addressed the requirement to report on its capability to carry

[3]Department of Defense, *Risk Management Guide for DOD Acquisition*, *6th Edition*, *Version 1.0* (August 2006); Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration for Development*, Version 1.2 (Pittsburgh, Pa., August 2006).

[4]We determined that a requirement was partially addressed if we identified shortcomings in the department's description of the actions taken to respond to the requirements, based on the information provided in DOD's report and best practices noted in our previously issued reports.

out necessary governance, management, and development functions of health information management and information technology systems.

- The department partially addressed the remaining 4 requirements, which pertained to identifying, assessing, and mitigating risks, as well as reporting on estimated resources required to optimally support health care information technology and planning corrective actions to remedy shortfalls that the department identified and reported. For example, the department had identified and assessed risk, but the report did not fully disclose these risks or the meaning of the department's assessment. Also, the report did not fully identify the staff and funds needed, nor did it fully identify the organizations responsible and accountable for accomplishing risk mitigation activities.

Conclusions

DOD provided the congressional defense committees with key information in response to the requirements that it report on such matters as assessment of its enterprise architecture, achievement of joint interoperability with VA, establishment of a virtual lifetime electronic record for members of the Armed Forces, analysis of departmental procurement methods, and evaluation of organizational management capabilities. While the department also reported information relative to the remaining four requirements, its reporting was only partially responsive to those requirements of the act pertaining to risk identification, assessment, and mitigation, as well as the estimated resources required to optimally support health care information technology and planned corrective actions to remedy shortfalls the department identified. If not addressed, DOD's incomplete reporting to address these requirements could impede the congressional defense committees' oversight of the department's planned improvements.

Recommendation for Executive Action

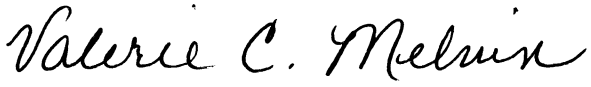
To address shortcomings in meeting these 4 reporting requirements, we recommend that the Secretary of Defense direct the Deputy Secretary of Defense to report to the congressional defense committees additional details to address shortcomings we identified for the reporting requirements regarding (1) risk identification and assessment, (2) risk mitigation planning, (3) corrective action planning, and (4) future year resources estimation.

Agency Comments and Our Evaluation

The Deputy Chief Management Officer, Office of the Deputy Secretary of Defense, provided written comments on a draft of this report. In its comments, the department agreed with our recommendation that it provide additional details about risks related to health information and information technology programs. Accordingly, the department included with its comments additional information that showed progress in addressing shortcomings identified in the report. The information included a description of each risk, risk level, and mitigation actions planned. Concerning the future year resources estimation, the department said that it would provide these additional details after the completion of the Electronic Health Record Way Ahead analysis of alternatives and approval of the Fiscal Year 2012 Program Objectives Memorandum submission. Providing these additional details should help ensure that the congressional defense committees have more complete information on risks and resource needs for achieving the timelines and goals of the department's health information and information technology programs. The department's comments are reprinted in appendix II.

We are sending copies of this report to interested congressional committees and the Secretary of Defense. In addition, the report will be available at no charge on GAO's Web site at http://www.gao.gov.

If you or your staffs have any questions concerning this report, please contact me at (202) 512-6304 or melvinv@gao.gov. Contact points for our Offices of Congressional Relations and Public Affairs may be found on the last page of this report. GAO staff who made major contributions to this report are listed in appendix III.



Valerie C. Melvin
Director, Information Management
and Human Capital Issues

List of Congressional Committees

The Honorable Carl Levin
Chairman
The Honorable John McCain
Ranking Member
Committee on Armed Services
United States Senate

The Honorable Daniel K. Inouye
Chairman
The Honorable Thad Cochran
Ranking Member
Subcommittee on Defense
Committee on Appropriations
United States Senate

The Honorable Tim Johnson
Chairman
The Honorable Kay Bailey Hutchison
Ranking Member
Subcommittee on Military Construction,
Veterans' Affairs, and Related Agencies
Committee on Appropriations
United States Senate

The Honorable Ike Skelton
Chairman
The Honorable Howard P. McKeon
Ranking Member
Committee on Armed Services
House of Representatives

The Honorable Norman D. Dicks
Chairman
The Honorable C.W. Bill Young
Ranking Member
Subcommittee on Defense
Committee on Appropriations
House of Representatives

The Honorable Chet Edwards
Chairman
The Honorable Zach Wamp
Ranking Member
Subcommittee on Military Construction,
Veterans Affairs, and Related Agencies
Committee on Appropriations
House of Representatives

Appendix I: Briefing for Staff Members of Congressional Committees

Department of Defense Health Care: Planned Improvements to the Governance and Execution of Supporting Information Management and Information Technology Programs

Briefing for Staff Members of Congressional Committees

July 23, 2010

Agenda

Introduction

Objective

Scope and Methodology

Results in Brief

Background

DOD's Reporting Requirements Identified in section 716 of the National Defense Authorization Act for Fiscal Year 2010

Conclusions

Recommendation for Executive Action

Agency Comments and Our Evaluation

Attachment 1: Congressional Addressees

2

Introduction

The National Defense Authorization Act for Fiscal Year 2010[1] included provisions directing the Department of Defense (DOD) to submit a report to congressional defense committees on improvements to the governance and execution of health information management and information technology (IT) programs planned and programmed to electronically support clinical medical care within the military health system.

In accordance with the act, DOD developed its report, entitled Improvements to the Governance and Execution of Health Information Management and Information Technology Programs. DOD submitted the report to the House and Senate Armed Services Committees and House and Senate Appropriations Committees on June 23, 2010.[2]

[1]Pub. L. No. 111-84, § 716 (2009).

[2]Although the report transmittal letters are dated June 21, 2010, according to the Office of the Deputy Chief Management Officer, the report was actually submitted to Congress on June 23, 2010.

3

Objective

The act directed GAO to assess DOD's report and plan of action to achieve the department's goals and mitigate risk in the management and execution of health information management and IT programs not later than 30 days after the report was submitted, and provide our results to the congressional defense committees.

Accordingly, our objective was to determine whether DOD addressed the reporting requirements specified in the act.

4

Scope and Methodology

To accomplish our objective, we

- reviewed DOD's reporting requirements set forth in section 716 of the National Defense Authorization Act for Fiscal Year 2010;
- reviewed DOD's report prepared in response to the act;
- reviewed our past work that examined DOD health information and technology issues, including reports that we issued in response to the National Defense Authorization Act for Fiscal Year 2008,[3] which discussed DOD's and the Department of Veterans Affairs' (VA) progress in implementing electronic health record systems;[4]

[3]Pub. L. No. 110-181, § 1635 (2008).

[4]GAO, *Electronic Health Records: DOD and VA Interoperability Efforts Are Ongoing; Program Office Needs to Implement Recommended Improvements*, GAO-10-332 (Washington, D.C.: Jan. 28, 2010) and *Electronic Health Records: DOD's and VA's Sharing of Information Could Benefit from Improved Management*, GAO-09-268 (Washington, D.C.: Jan. 28, 2009).

5

Scope and Methodology

- reviewed DOD risk management guidance and Software Engineering Institute guidance;[5]
- determined whether requirements were addressed or partially addressed (we determined that a requirement was partially addressed if we identified shortcomings in the department's description of the actions taken to respond to the requirements, based on the information provided in DOD's report and best practices noted in our previously issued reports); and
- discussed our determinations with the Office of the Deputy Chief Management Officer.

[5]Department of Defense, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0* (August 2006); Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration for Development, Version 1.2* (Pittsburgh, Pa., August 2006).

6

Scope and Methodology

We conducted this performance audit from June 2010 to July 2010, in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

7

Results in Brief

DOD addressed six of the ten reporting requirements included in section 716 of the National Defense Authorization Act for Fiscal Year 2010. For example, the department addressed the requirement to report on its capability to meet requirements for joint interoperability with the Department of Veterans Affairs. Also, the department addressed the requirement to report on its capability to carry out necessary governance, management, and development functions of health information management and information technology systems.

The department partially addressed the remaining four requirements, which pertained to identifying, assessing, and mitigating risks, as well as reporting on estimated resources required to optimally support health care information technology and planning corrective actions to remedy shortfalls that the department identified and reported. If not corrected, DOD's incomplete reporting to address these requirements could impede the congressional defense committees' oversight of the department's planned improvements.

We are recommending that the Deputy Secretary of Defense report to the congressional defense committees additional details to address the shortcomings that we identified for these four requirements. In oral comments on a draft of this briefing, DOD's Deputy Chief Management Officer concurred with our recommendation and described actions to address shortcomings that we identified for the reporting requirements.

8

Background

DOD plans to improve the quality of health care provided to service members and their beneficiaries through the refinement and increased sharing of electronic health records. The department's strategy includes initiatives to modernize current electronic health record capabilities and stabilize legacy systems serving as its platform for interoperability. It has identified the Electronic Health Record (EHR) Way Ahead as the department's effort to improve the accuracy and completeness of its electronic health data, improve the exchange of electronic health information with VA, and support electronic medical data capture and exchange between private health care providers, and state, local, and other federal agencies.

The department has also stated that it plans to expand its sharing of information captured in its electronic health record through such efforts as implementation of the Virtual Lifetime Electronic Record (VLER), an initiative to enable DOD, VA, and other government entities to exchange electronic health record information with each other and with private sector health care providers; and by leveraging the Nationwide Health Information Network, an Internet-based capability enabling Web-based, secure exchange of health information.

9

Background

We have previously reported on DOD's longstanding efforts to modernize its health information systems and its efforts toward increasing its sharing of electronic health records. Among other matters, our work has noted challenges that the department has faced in achieving joint electronic health record interoperability with VA. We have made various recommendations aimed at improving the two departments' health information technology and information-sharing efforts. The departments have generally agreed with our recommendations.

Reflecting congressional concern with DOD's efforts to improve its health information technology programs, section 716 of the National Defense Authorization Act for Fiscal Year 2010 required the Deputy Secretary of Defense (as the department's Chief Management Officer) to submit a report to Congress on the improvements that DOD is making to the governance of its health information management and information technology programs.

The act identified 10 requirements on which DOD was to report, as listed in table 1 below.

10

Background

Table 1: DOD Reporting Requirements in Section 716 of the National Defense Authorization Act for Fiscal Year 2010

DOD reporting requirements
(1) An assessment of the capability of the enterprise architecture to achieve optimal clinical practices and health care outcomes.
(2) For each health information management and information technology program covered by the report, an identification and assessment of the risks associated with achieving the timelines and goals of the program.
(3) A plan of action to mitigate the risks identified.
(4) An assessment of the appropriateness of the health information management and IT technical architecture and whether that architecture leverages the current best practices of industry, including the ability to meet the interoperability standards required by § 1635 of the Wounded Warrior Act (title XVI of Pub. L. No. 110-181; 10 U.S.C. 1071 note), as amended by § 252 of the Duncan Hunter National Defense Authorization Act for Fiscal Year 2009 (Public Law 110-417; 122 Stat. 4400).
(5) An assessment, in coordination with the Secretary of Veterans Affairs, of (a) the capability of DOD of meeting the requirements for joint interoperability with the Department of Veterans Affairs, as required by such section 1635, and (b) the progress the Secretary of Defense and the Secretary of Veterans Affairs have made on the establishment of a joint virtual lifetime electronic record for members of the Armed Forces.
(6) A plan to take corrective actions that are necessary to remedy shortfalls identified as a result of the assessments.

11

Background

DOD Reporting Requirements
(7) An assessment of the estimated resources required in future years to achieve optimal information technology support for health care clinical practice and quality and compliance with the requirements of such section 1635.
(8) An analysis of the methods by which the Office of the Assistant Secretary of Defense for Health Affairs procures health information management and information technology goods and services, and of the appropriateness of the application of legal and acquisition authorities.
(9) An analysis of the capabilities of the Office of the Assistant Secretary of Defense for Health Affairs to carry out necessary governance, management, and development functions of health information management and information technology systems, including (a) the recommendations of the Assistant Secretary for improvements to the Office or alternative organizational structures for the Office, and (b) alternative organizations within the Department of Defense with equal or greater management capabilities for health information management and information technology.
(10) A recommendation as to whether health information management and IT systems of DOD should be included in and subject to the requirements of section 2222 of Title 10, United States Code.

Source: GAO analysis of sec. 716 of the National Defense Authorization Act for FY 2010.

12

Background

In June 2010, the Deputy Secretary of Defense submitted the report required by section 716 of the act to the congressional defense committees, addressing improvements to the governance and execution of DOD health information management and IT programs.

13

Background

To address the requirements set forth in the act, DOD stated in its report that it performed assessments of the department's activities in three categories and an independent third party assessed activities in a fourth category:

- A **functional and technical assessment** explored risks associated with closing current capability gaps and satisfying known requirements, as well as those related to system architecture and standards maturity. This assessment was intended to address requirements 1, 2, 3, and 4.
- A **joint interoperability assessment** addressed the progress of DOD's interagency interoperability efforts, investigated risks associated with coordinating activities between DOD and VA, and evaluated progress of the VLER initiative. This assessment was intended to address requirement 5.
- A **program management assessment** identified risks associated with overall execution, funding, program schedules, and resource dependencies. This assessment was intended to address requirements 7, 8, and 10.
- An **organizational assessment**, performed by an independent third party, outlined risks associated with governance, oversight authorities, reporting structures, and culture change within the DOD entity responsible for managing health affairs. This assessment was intended to address requirement 9.

14

Background

In addition, DOD included in its report an appendix that summarized risks, mitigations, and milestones, which the department described as a corrective action plan to improve its EHR applications and supporting infrastructure. This information was intended to address requirement 6.

15

Reporting Requirement 1

An assessment of the capability of the enterprise architecture to achieve optimal clinical practices and health care outcomes.

DOD addressed this requirement by reporting that it performed a functional and technical assessment of the enterprise architecture (EA) for the department's new electronic health record, referred to as the EHR Way Ahead. This assessment was to determine whether the architecture addresses requirements and gaps between existing and desired capabilities. The department concluded that the EHR Way Ahead EA was sufficient to realize initial capabilities and desired outcomes.

16

Reporting Requirement 2

For each health information management and information technology program covered by the report, an identification and assessment of the risks associated with achieving the timelines and goals of the program.

DOD partially addressed this requirement. Specifically, DOD reported summary information on risks, selected risk statements, mitigation plans, and milestones. For example, it reported the results of its functional assessment of the architecture (i.e., whether the architecture addresses capability gaps), identifying 17 high, 12 medium, and 38 low risks; it also reported the results of its technical assessment of the architecture, which identified 2 high, 27 medium, and 7 low risks. However, a complete listing of these risks, definitions of risk levels (i.e., high, medium, and low), and assessments of each risk's level (as called for in DOD's and the Software Engineering Institute's guidance[6]) were not reported. Thus, while DOD has identified and assessed risks, the report does not fully disclose these risks or the meaning of the department's assessment. As a result, it does not provide the congressional defense committees with a complete view of the risks and related assessments associated with achieving the timelines and goals of DOD's health information management and information technology programs.

[6]Department of Defense, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0* (August 2006); Carnegie Mellon Software Engineering Institute, *Capability Maturity Model Integration for Development, Version 1.2* (Pittsburgh, Pa., August 2006).

17

Reporting Requirement 3

A plan of action to mitigate the risks identified.

The department partially addressed this requirement because fully addressing the requirement is largely dependent on the identification and assessment of risks, as called for in reporting requirement 2. The department reported summary information on its risk mitigation plans and milestones. However, the reported plan of action to mitigate risks does not include all the elements of an effective plan (e.g., identification of resource needs and responsible parties), as described in DOD's risk management guidance.[7] In particular, the report did not fully identify the staff and funds needed, nor did it fully identify the organizations that are responsible and accountable for accomplishing risk mitigation activities. As a result, DOD's report does not provide the congressional defense committees with complete information about the department's plans to mitigate risks to its health information management and information technology programs.

[7]Department of Defense, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0* (August 2006).

18

Reporting Requirement 4

An assessment of the appropriateness of the health information management and IT technical architecture and whether that architecture leverages the current best practices of industry.

The department addressed this requirement by reporting that its EHR technical architecture, although in the early stages of maturity, was compliant with the DOD Information Enterprise Architecture at a high level, while acknowledging the need to further develop specific engineering and implementation architecture content. Further, the department reported that the EHR technical architecture was compliant with the DOD Net-Centric Data and Services Strategy. According to the department, its assessment determined that the EHR technical architecture was consistent with relevant best practices, DOD policy, and interoperability standards.

19

Reporting Requirement 5

Determine the capability of DOD of meeting the requirements for joint interoperability with the Department of Veterans Affairs and the progress made on the establishment of a joint virtual lifetime electronic record for members of the Armed Forces.

The department addressed this requirement by conducting an assessment that focused on progress toward increased sharing of electronic health records between DOD and VA, as required by the National Defense Authorization Act for Fiscal Year 2008.[8] To increase sharing of electronic health records between the departments, DOD and VA established six interoperability objectives (such as demonstrating an initial capability to scan documents). DOD's report described both departments' efforts to meet all six of their objectives and stated that they consider achievement of these objectives, in conjunction with other capabilities previously achieved,[9] to be sufficient to address the act.

[8]Pub. L. No. 110-181, § 1635 (2008). The act required DOD and VA to jointly develop and implement electronic health record systems or capabilities that allow for full interoperability of personal health care information by September 30, 2009.

[9]DOD and VA have identified these other previous capabilities as being the Federal Health Information Exchange, the Bidirectional Health Information Exchange, and the DOD Clinical Data Repository/VA Health Data Repository.

20

Reporting Requirement 5 (cont.)

In January 2010,[10] we reported that although the departments had achieved planned capabilities for all six of their interoperability objectives, the departments were planning additional actions to further increase their capabilities for allowing interoperability, in recognition that clinicians' needs for interoperable electronic health records are evolving. For example, DOD and VA stated that they planned to meet additional needs with respect to social history and physical exam data.

Further, DOD's report stated that the James A. Lovell Federal Health Care Center in North Chicago will "revolutionize" interoperability between DOD and VA, delivering reusable capabilities to register patients and process orders between the health systems of both departments. We have ongoing work that is examining this initiative.

[10]GAO-10-332.

Reporting Requirement 5 (cont.)

In addition, to address the requirement, the department described progress and plans for developing VLER. In this regard, DOD stated that the departments have successfully begun implementing this initiative in measurable phases. For example, it stated that the departments conducted Phase 1a in December 2009 and January 2010, by enabling the exchange of selected patient health data between DOD, VA, and a private health care provider in San Diego, California. Further, the department reported on its plans for implementing VLER, noting, for example, its intent to demonstrate the capability to exchange laboratory data in the Tidewater area of Southeastern Virginia between DOD, VA, and a private sector partner by July 31, 2010. The report highlighted that the departments will continue to develop plans for future pilots, with a goal of national deployment by December 2012.

We have work ongoing that is examining the VLER initiative.

22

Reporting Requirement 6

Develop a plan to take corrective actions that are necessary to remedy shortfalls identified as a result of the assessments.

The department partially addressed this requirement by including in its report an appendix (appendix B) that included summary information on risks, planned mitigation steps, and information on milestones for the four assessment categories. However, the appendix did not fully address basic elements of an effective risk mitigation plan, such as the identification of responsible parties and resources needed to execute the plan, as described in DOD's risk management guidance.[11] As a result, the congressional committees were not provided with a complete plan that DOD intends to execute to remedy the shortfalls identified in its assessment.

[11]Department of Defense, *Risk Management Guide for DOD Acquisition, 6th Edition, Version 1.0* (August 2006).

23

Reporting Requirement 7

An assessment of the estimated resources required in future years to achieve optimal information technology support for health care clinical practices and quality and compliance with applicable requirements.

The department partially addressed this requirement. The department reported that it reviewed budget requests to determine if sufficient resources were available or identified for its EHR needs. It stated that its fiscal year 2011 budget request included $302 million for the EHR modernization program and $40 million for the VLER initiative. Further, the department said that the fiscal year 2012 appropriation mix may be revised based upon the results of its EHR Way Ahead analysis of alternatives and after issuance of the approved Acquisition Decision Memorandum. However, the department did not provide an assessment of the estimated resources for future years to procure technology goods and services, as called for in this requirement. As a result, the congressional committees were not provided with a complete assessment of the estimated resources required in future years to achieve optimal health care information technology support.

24

Reporting Requirement 8

An analysis of methods by which the Assistant Secretary of Defense for Health Affairs procures health information management and information technology goods and services, and of the appropriateness of the application of legal and acquisition authorities.

The department addressed this requirement by evaluating its contracting and acquisition processes relative to relevant statutes (e.g., the Weapon Systems Acquisition Reform Act of 2009 and the Clinger-Cohen Act of 1996) and DOD acquisition policy. The department reported that its assessment revealed no deficiencies in procurement methods for the EHR and determined that the methods were legally sound and in accordance with DOD policy.[12]

[12]We have identified DOD contracting in our High-Risk List since 1992 and DOD business systems modernization as high risk since 1995; however, we did not explicitly identify DOD's health care information technology procurement processes as a high risk area. See GAO, *High-Risk Series: An Update*, GAO-09-271 (Washington, D.C.: Jan. 22, 2009).

25

Reporting Requirement 9

An analysis of the capabilities of the Office of the Assistant Secretary of Defense for Health Affairs to carry out necessary governance, management, and development functions of health information management and information technology systems, including the recommendations of the Assistant Secretary for improvements to the Office or alternative organizational structures for the Office and alternative organizations within DOD with equal or greater management capabilities for health information management and information technology.

The department addressed this requirement by tasking an independent organization, the Institute for Defense Analysis, to assess capabilities of the Office of the Assistant Secretary of Defense for Health Affairs. According to DOD's report, the study team used a previously developed framework and document reviews and interviews to identify and assess the functions necessary for governance, management, and development of health information technology and information technology systems. The report included the team's observations in these areas. The team also identified, from prior studies and activities concerning other organizations within DOD, existing organizations within the department that might have equal or greater management capabilities for health information management and information technology.

26

Reporting Requirement 10

A recommendation as to whether health information management and information technology systems of DOD should be included in and subject to the requirements of section 2222 of Title 10, United States Code.

The department addressed this requirement by recommending that health information technology systems be included in and subject to the requirements of section 2222 of Title 10, United States Code, thus concluding that the EHR is to be managed as a "Defense Business System" rather than as a "National Security System."

27

Conclusions

DOD provided the congressional defense committees with key information in response to the requirements that it report on such matters as assessment of its enterprise architecture, achievement of joint interoperability with the Department of Veterans Affairs, establishment of a virtual lifetime electronic record for members of the Armed Forces, analysis of departmental procurement methods, and evaluation of organizational management capabilities. While the department also reported information relative to the remaining four requirements, its reporting was only partially responsive to requirements of the act pertaining to risk identification, assessment, and mitigation, as well as the estimated resources required to optimally support health care information technology and planned corrective actions to remedy shortfalls the department identified. If not addressed, DOD's incomplete reporting to address these requirements could impede the congressional defense committees' oversight of the department's planned improvements.

28

Recommendation for Executive Action

We are recommending that the Deputy Secretary of Defense report to the congressional defense committees additional details to address the shortcomings that we identified for the reporting requirements regarding

- risk identification and assessment,
- risk mitigation planning,
- corrective action planning, and
- future year resources estimation.

29

Agency Comments and Our Evaluation

In oral comments on a draft of the briefing slides, DOD's Deputy Chief Management Officer concurred with our recommendation and described actions to address shortcomings that we identified for the reporting requirements. For example, the official stated that the department would provide the congressional committees with more detailed information regarding its risk identification, assessment, and mitigation planning, including risk levels and responsible organizations and resources. The official also stated that DOD would update the corrective action plan to identify responsible organizations and resources needed to execute the plan. Further, the official stated that, following the selection and approval of a technical solution for the EHR Way Ahead, and approval of the Fiscal Year 2012 Program Objectives Memorandum, the department would provide future-years resource estimates. Providing this additional information should better inform the congressional committees' oversight of DOD's planned improvements.

30

Attachment 1
Congressional Addressees

Committee on Armed Services
United States Senate

Subcommittee on Defense
Committee on Appropriations
United States Senate

Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Committee on Appropriations
United States Senate

Committee on Armed Services
House of Representatives

Subcommittee on Defense
Committee on Appropriations
House of Representatives

Subcommittee on Military Construction, Veterans Affairs, and Related Agencies
Committee on Appropriations
House of Representatives

31

Appendix II: Comments from the Department of Defense

DEPUTY CHIEF MANAGEMENT OFFICER
9010 DEFENSE PENTAGON
WASHINGTON, DC 20301-9010

NOV 9 2010

Ms. Valerie C. Melvin
Director, Information Management and
Human Capital Issues
U.S. Government Accountability Office
441 G Street, NW
Washington, DC 20548

Dear Ms. Melvin:

The Department of Defense (DoD) response to the Government Accountability Office's (GAO) draft report 11-148, "HEALTH INFORMATION TECHNOLOGY: DoD Needs to Provide More Information on Risks to Improve Its Program Management," dated October 14, 2010 (GAO Code 310959 Formerly GAO Code 310954) is contained in this letter. The Department concurs with GAO's recommendation contained in the draft report.

Your audit highlighted the need for DoD to provide additional details regarding risk identification and assessment, risk mitigation planning, corrective action planning and future year resources estimation. Accordingly, an enhanced mitigation plan which includes a complete listing of risks, risk level definitions and an assessment of each risk's level is included at TAB A. The attached mitigation plan also identifies organizations responsible for risk mitigation activities and estimated resource needs.

Additional details regarding future year resource estimates will be provided upon completion of the Electronic Health Record Way Ahead Analysis of Alternatives and approval of the Fiscal Year 2012 Program Objectives Memorandum submission.

Sincerely,

Elizabeth A. McGrath

Attachment:
As stated

Appendix III: GAO Contact and Staff Acknowledgments

GAO Contact

Valerie C. Melvin at (202) 512-6304 or melvinv@gao.gov

Staff Acknowledgments

In addition to the individual named above, key contributions were made to this report by Cynthia Scott (Assistant Director), Mark Bird, Kelly Dodson, Lee McCracken, Donald Sebers, Matthew Snyder, Daniel Wexler, and Robert L. Williams, Jr.

GAO's Mission

The Government Accountability Office, the audit, evaluation, and investigative arm of Congress, exists to support Congress in meeting its constitutional responsibilities and to help improve the performance and accountability of the federal government for the American people. GAO examines the use of public funds; evaluates federal programs and policies; and provides analyses, recommendations, and other assistance to help Congress make informed oversight, policy, and funding decisions. GAO's commitment to good government is reflected in its core values of accountability, integrity, and reliability.

Obtaining Copies of GAO Reports and Testimony

The fastest and easiest way to obtain copies of GAO documents at no cost is through GAO's Web site (www.gao.gov). Each weekday afternoon, GAO posts on its Web site newly released reports, testimony, and correspondence. To have GAO e-mail you a list of newly posted products, go to www.gao.gov and select "E-mail Updates."

Order by Phone

The price of each GAO publication reflects GAO's actual cost of production and distribution and depends on the number of pages in the publication and whether the publication is printed in color or black and white. Pricing and ordering information is posted on GAO's Web site, http://www.gao.gov/ordering.htm.

Place orders by calling (202) 512-6000, toll free (866) 801-7077, or TDD (202) 512-2537.

Orders may be paid for using American Express, Discover Card, MasterCard, Visa, check, or money order. Call for additional information.

To Report Fraud, Waste, and Abuse in Federal Programs

Contact:

Web site: www.gao.gov/fraudnet/fraudnet.htm
E-mail: fraudnet@gao.gov
Automated answering system: (800) 424-5454 or (202) 512-7470

Congressional Relations

Ralph Dawn, Managing Director, dawnr@gao.gov, (202) 512-4400
U.S. Government Accountability Office, 441 G Street NW, Room 7125
Washington, DC 20548

Public Affairs

Chuck Young, Managing Director, youngc1@gao.gov, (202) 512-4800
U.S. Government Accountability Office, 441 G Street NW, Room 7149
Washington, DC 20548