UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Carl Levin
Chairman
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the other congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable John McCain
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Jim Webb
Chairman
Subcommittee on Personnel
Committee on Armed Services
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Lindsey Graham
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Howard P. "Buck" McKeon
Chairman
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the other congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Adam Smith
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Joe Wilson
Chairman
Subcommittee on Military Personnel
Committee on Armed Services
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Susan A. Davis
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Daniel K. Inouye
Chairman
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the other congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383)—and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Vice Chairman

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Daniel K. Inouye
Chairman
Subcommittee on Defense
Committee on Appropriations
United States Senate
Washington, DC 20510

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Thad Cochran
Vice Chairman

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable Harold Rogers
Chairman
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the other congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member

UNDER SECRETARY OF DEFENSE
4000 DEFENSE PENTAGON
WASHINGTON, DC 20301-4000

PERSONNEL AND
READINESS

APR 3 2012

The Honorable C.W. Bill Young
Chairman
Subcommittee on Defense
Committee on Appropriations
U.S. House of Representatives
Washington, DC 20515

Dear Mr. Chairman:

I am pleased to forward the enclosed report on the Department of Defense (DoD) enterprise architecture to guide the transition of the electronic health record (EHR), and related matters, as required by section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81). This issue falls under my purview, and I have been asked to respond. A similar letter is being sent to Chairmen of the congressional defense committees.

The report addresses the architecture to guide the transition of the DoD EHR to a future state that is cost-effective and interoperable. To do so, the Secretary of Defense and Secretary of Veterans Affairs (VA) are committed to pursuing a joint, common platform enabled through appropriate governance for the EHR. The Departments already have identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The report also discusses a process for selecting investments in information technology—the report requested by section 715 of the Ike Skelton NDAA for FY 2011 (P.L. 111-383) —and the role of the DoD/VA Interagency Program Office to manage or oversee efforts with respect to the future EHR program.

Thank you for your interest in the health and well-being of our Service members, veterans, and their families.

Sincerely,

Jo Ann Rooney
Acting

Enclosure:
As stated

cc:
The Honorable Norman D. Dicks
Ranking Member

Report to Congressional Defense Committees on

Department of Defense Enterprise Architecture to Guide the Transition of the DoD Electronic Health Record, and Related Matters

In response to
Section 717 of the National Defense Authorization Act for Fiscal Year 2012
and including a response to
Section 715(a) of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011

Preparation of this report cost the Department of Defense
a total of approximately $31,000 for Fiscal Year 2012

Department of Defense Enterprise Architecture to Guide the Transition of the DoD Electronic Health Record, and Related Matters

TABLE OF CONTENTS

EXECUTIVE SUMMARY 1

I. THE ENTERPRISE AND ITS ARCHITECTURE 3

A. Institutional Commitment to the iEHR Initiative and the iEHR Enterprise Architecture 3

1. The iEHR Initiative 3
2. iEHR Enterprise Architecture 4

B. Governance Foundation of the iEHR Enterprise Architecture 5

1. Functional Capabilities Planning Group (FCPG) and Capability Integrated Product Team (C-IPT) 5
2. Advisory Bodies 5
   a. DoD/VA Interagency Clinical Informatics Board (ICIB) 6
   b. VA/DoD Health Executive Council (HEC) Information Management / Information Technology (IM/IT) Workgroup (WG) 7
   c. Health Architecture Review Board (HARB) 7
3. VA/DoD Health Executive Council (HEC) 8
4. IPO Advisory Board 9
5. VA/DoD Joint Executive Council (JEC) 9
6. Senior Military Medical Advisory Council (SMMAC) 9

C. Management Foundation for the iEHR Enterprise Architecture 9

D. Development of Initial Versions of the iEHR Enterprise Architecture 10

1. Functional and Technical Assessment of the Electronic Health Record Way Ahead (EHRWA) Enterprise Architecture 10
2. Foundation of the iEHR Enterprise Architecture 11
   a. Enterprise Service Bus (ESB) 11
   b. DoD Data Model Mapping 12
   c. Identity Management 12
   d. DoD/VA Data Center Consolidation and Cloud Computing 14
3. Transition Planning 16
   a. Transition Application Plan (TAP) 16
   b. Transition Planning Methodology and Management 17

II. INVESTMENT 18

A. iEHR Enterprise Architecture 18

1. Program Performance 18

2. IT Resource Planning and Allocation 19

3. Contribution to Interoperability 19

B. Cost Assessment and Program Evaluation (CAPE) Office 19

C. Technical Approach 19

D. Governance Model / Charters 20

E. Health Architecture Review Board (HARB) 20

F. Enterprise Architecture Management Plan (EAMP) 20

G. Conceptual Architecture 20

H. iEHR Functional Capability Sets 21

III. REPORTING UNDER SECTION 715 OF THE IKE SKELTON NDAA FY 2011 22

A. The Ike Skelton NDAA FY 2011, Section 715(c) 22

B. The Ike Skelton NDAA FY 2011, Section 715(b) 23

C. The Ike Skelton NDAA FY 2011, Section 715(a) 23

1. Prior Related Reports 23

2. Foundation of Risk Management for Defense Acquisition 24

a. Defense Acquisition Guidebook 24

b. Risk Management Guide for DoD Acquisition 31

3. Application of Risk Management Methodologies to HIT Acquisition 31

4. Risk Assessment under the iEHR Enterprise Architecture 32

IV. DOD/VA INTERAGENCY PROGRAM OFFICE (IPO) 32

V. CONCLUSION 33

ACRONYMS AND ABBREVIATIONS I

EXHIBIT A – IPO CHARTER

Department of Defense Enterprise Architecture to Guide the Transition of the DoD Electronic Health Record, and Related Matters

This report responds to the requirement in section 717 of the National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2012 (P.L. 112-81) (NDAA FY 2012), which states:

> SEC. 717. LIMITATION ON AVAILABILITY OF FUNDS FOR THE FUTURE ELECTRONIC HEALTH RECORDS [EHR] PROGRAM.
>
> (a) LIMITATION.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2012 for the procurement, research, development, test, and evaluation, or operation and maintenance of the future electronic health records program, not more than 10 percent may be obligated or expended until the date that is 30 days after the date on which the Secretary of Defense submits to the congressional defense committees a report addressing—
>
> (1) an architecture to guide the transition of the electronic health records of the Department of Defense [DoD] to a future state that is cost-effective and interoperable;
>
> (2) the process for selecting investments in information technology [IT] that support the architecture described in paragraph (1);
>
> (3) the report required by section 715 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111-383; 124 Stat. 4249);
>
> (4) the role of the Interagency Program Office [IPO] to manage or oversee efforts with respect to the future electronic health records program; and
>
> (5) any other matters the Secretary considers appropriate.
>
> (b) FUTURE ELECTRONIC HEALTH RECORDS PROGRAM DEFINED.—In this section, the term "future electronic health records program" means the programs of the Department of Defense referred to as the "EHR way ahead" [EHRWA] and the "virtual lifetime electronic record [VLER]."

Executive Summary

OVERVIEW: Part I of this report discusses development of the enterprise architecture (EA) that will guide the transition of DoD's EHR to a future state that is cost-effective and interoperable. Part II focuses on the process for selecting IT investments to support the EA. Part III reports the status of related reports required under the Ike Skelton NDAA FY 2011, section 715. Part IV addresses the management and oversight role of the IPO with respect to the integrated Electronic Health Record (iEHR) EA. Finally, Part V contains the report's concluding statements.

SUMMARY: DoD and the Department of Veterans Affairs (VA) (Departments) are committed to providing the highest quality healthcare to their beneficiaries. To advance the goal of achieving

a joint iEHR, the Departments have embarked on the collaborative development of the necessary EA. The iEHR EA will be based on architecture work already completed in each Department. It will provide for a systematic approach to support the alignment of enterprise resources and investments with enterprise-wide business needs and programs to achieve the iEHR.

Faced with a mutual need to modernize legacy EHR systems, the Departments have agreed to implement a joint, common EHR platform, purchasing commercially available components for joint use whenever possible and cost effective. In order to execute this agreement, governance and management structures have been put in place or modified to support both the iEHR and VLER Health. These structures include a combined requirements generation process leveraging a re-chartered DoD/VA Interagency Clinical Informatics Board (ICIB) and VA/DoD Health Executive Council (HEC); a new Health Architecture Review Board (HARB); a re-chartered and more empowered DoD/VA Interagency Program Office (IPO); and a new IPO Advisory Board.

EA Approach and Management: The EA effort provides for a systematic approach to support the alignment of enterprise resources and investments with enterprise-wide business needs and programs to achieve iEHR and VLER Health objectives. The Departments are merging the iEHR and VLER Health EA efforts of the Departments to advance their goals. To foster innovation and expedite the delivery of products to the user, the iEHR will leverage both open source and traditional approaches to software acquisition. The IPO will coordinate with the Departments as the iEHR architecture matures throughout the acquisition process. The new HARB will oversee development and life-cycle management of combined EA efforts.

The iEHR EA will rest on a strong management foundation in the re-chartered IPO. The IPO will include a senior Technical Director, a senior Chief Architect, and a senior Director of Engineering, Development and Testing (ED&T); these leaders will ensure that the iEHR and VLER Health are guided by a robust EA. The iEHR and VLER Health project teams will be led by seasoned and certified program managers (PMs), with a matrixed support team of experienced architectural and engineering personnel.

Staffing Efforts: Barclay Butler, PhD, was appointed to the position of IPO Director effective February 27, 2012. On the same day, the interim Deputy Director, Stanley Lowe was named the permanent Deputy Director. The Departments are completing position descriptions and transfer packages for personnel identified for initial placement within the IPO. The EHRWA Planning Office personnel were realigned under IPO effective January 29, 2012.

The Departments have assigned full-time PMs for iEHR and VLER Health. The DoD Program Executive Officer (PEO) of Joint Medical Information Systems (JMIS) was detailed to the IPO effective February 13, 2012, to serve as interim Technical Director during the standup of the reorganized IPO. The Chief Technical Officer (CTO) of the Military Health System (MHS) Office of the Chief Information Officer is performing the duties of Chief Architect of the IPO. The Director of ED&T has been detailed from VA to the IPO and has begun comprehensive engineering planning efforts in coordination with the IPO Technical Director, Chief Architect and PMs.

Transition Management: DoD is establishing a small and focused transition office to assist the IPO and the legacy system management transition from current system-centric architectures to modern net-centric service oriented architecture (SOA). The transition office will work closely with DoD enterprise stakeholders to help coordinate the investment portfolio and ensure that transition strategies are clinically relevant, technically feasible, and financially viable.

The ultimate objective of the iEHR EA is to ensure delivery of the right information, to the right people, at the right time, with the best value for our healthcare beneficiaries.

I. The Enterprise and its Architecture

A. Institutional Commitment to the iEHR Initiative and the iEHR Enterprise Architecture

1. The iEHR Initiative

The Departments are institutionally committed to establishing and refining an iEHR, and to aligning resources and investments with business needs and programs across enterprises. On June 23, 2011, the Secretaries of the Departments approved a joint approach to iEHR and an effective governance structure to oversee the effort. The envisioned target state of the iEHR features:

- Joint use of the iEHR to help contain healthcare costs and provide higher value-based healthcare delivery systems;
- A coordinated "best-of-breed" approach that includes a mix of existing SOA-compliant capabilities, commercial off-the-shelf, open source, and custom systems;
- Use of agile development that will allow the Departments to deliver capabilities to customers at a more rapid pace; and
- Operation of the IPO as the single point of accountability for the iEHR initiative and VLER Health.

Additional core agreements, applicable across enterprises, include:

- Alignment to a common data model that includes common terminology models, data exchange specifications, common standards, and translation services to ensure data interoperability;
- Designation of the Defense Manpower Data Center as the single "identity management" source;

- Use of common data centers run by the Defense Information Systems Agency (DISA), based on cost and service level agreements;
- Acquisition of a common enterprise service bus (ESB) and use of a shared common service broker (CSB) approach;
- Development of a common presentation layer;
- Use of common measures of success and establishment of standard end-to-end business processes; and
- Development of Department-unique capabilities utilizing standardized application protocol interfaces (APIs) that will accommodate future adoption by other Government departments or agencies.

2. iEHR Enterprise Architecture

At the foundation of the iEHR initiative, the Departments are creating an iEHR EA, which is a conceptual blueprint that defines the structure and operation of the initiative and provides the basis to determine how the Departments can effectively achieve their current and future objectives. The iEHR EA describes the Departments' core mission, details each component needed to perform that mission, and illustrates how these components are interrelated. The iEHR EA will be based on architecture work already completed in each Department. It will provide for a systematic approach to support the alignment of enterprise resources and investments with enterprise-wide business needs and programs to achieve an iEHR.

The iEHR Enterprise Architecture Management Plan (EAMP) (version 1.0 published jointly in July 2011) defines the role of EA within the iEHR, and the EA's associated stakeholders and governance bodies; describes the current joint EA; and articulates the process by which future joint EA products will be developed. The iEHR EAMP outlines the iEHR EA program and the Departments' intention to align and unify DoD/VA strategic initiatives, business processes, information flows, systems and services, and technology infrastructure. The shared objective is to ensure that all major initiatives, processes, projects, IT standards, and investments support DoD/VA stated mission, vision, and strategic goals. Joint approval of the EAMP is expected by the third quarter of FY 2012.

The baseline iEHR architecture is the MHS EHRWA architecture; this architecture has been under development, evolution, and evaluation for a number of years. In early 2011, the Departments agreed that MHS EHRWA architecture would be the "presumptive" architecture. It has since evolved into the target iEHR EA based on identified joint functional capabilities.

The goal of the iEHR EA is to explicitly and formally define the EA for the enterprise, which will enable the Departments to respond to change and perform their operations in the most integrated, efficient and effective manner. The Departments have defined the organizational

process through which to develop, manage, oversee, approve, and disband capabilities to support the iEHR initiative.

Elements of the iEHR initiative are characterized in the Enterprise Conformance and Compliance Framework (ECCF) as being conceptual, logical or implementable. During the conceptual phase, the Departments developed a governance foundation for the iEHR, which is discussed below in Part B.

B. Governance Foundation of the iEHR Enterprise Architecture

The Departments' institutional commitment to the iEHR EA is evident in the governance structure established to direct resources. These resources, which include information management and information technology (IM/IT) resources, will be directed to investments and projects that will meet the needs of customers and stakeholders, and will have the greatest positive impact on the performance of the iEHR. Through a joint governance structure staffed with experienced leaders, the Departments are identifying and tackling any cultural barriers to the iEHR initiative. The iEHR EA governance structure—adopted in the conceptual phase—is documented in the EAMP.

A description of the governance structure's essential features, beginning at its foundation, follows.

1. Functional Capabilities Planning Group (FCPG) and Capability Integrated Product Team (C-IPT)

The DoD/VA functional community leads the requirements development process through the FCPG, under the guidance of the ICIB. The FCPG identifies and defines proposed joint functional capabilities, then orients baseline architectural artifacts within the logical construct of the ECCF. A C-IPT—guided by the ECCF—re-engineers joint functional processes and supplements the descriptive content of architectural artifacts, as needed. Ultimately, the FCPG is responsible for developing business standards for managing information integration and knowledge sharing across the care continuum to support the delivery of integrated healthcare.

2. Advisory Bodies

Architectural artifacts are submitted by the FCPG to three advisory bodies, whose responsibilities span the Departments' iEHR initiative: the ICIB, HEC IM/IT Workgroup (WG) (HEC IM/IT WG), and HARB. The governance function of each body is described below. The roles and responsibilities of these groups, and their placements within the governance structure, may change as governance processes mature.

a. DoD/VA Interagency Clinical Informatics Board (ICIB)

The ICIB is an advisory board that considers proposed joint capabilities and provides functional validation. Composed of functional leaders from the Departments, including Service leaders, the ICIB identifies and recommends priorities of strategic clinical capabilities that drive acquisition and support of health information systems. The ICIB's authority to make recommendations embraces clinical capabilities, such as clinical decision support (CDS). The ICIB makes its recommendations to the HEC regarding the development, implementation, evaluation, and management of the iEHR and health information exchanges between and among the Departments and other Federal and private sector partners. The ICIB identifies, prioritizes, and validates business functional requirements ensuring efficient provider workflows and effective clinical processes. The ICIB also engages actively in clinical system testing, implementation, and performance monitoring activities.

As the Departments engaged the iEHR initiative in 2011, healthcare providers in the ICIB were identified as key functional stakeholders to lead the initial focus teams defining the program. ICIB members were co-chairs of focus teams in the areas of systems capabilities, mission requirements and performance outcomes, business requirements, and the iEHR presentation layer. These members also supported a data interoperability focus team. Ultimately, ICIB providers were co-chairs or key members in five of the six focus teams dedicated to the iEHR. These teams—from both Departments—defined a list of more than 30 functional capabilities to support an iEHR, as well as the governance structure to guide the capability development lifecycle.

The ICIB members are key players in the iEHR governance structure, which highlights processes, roles and responsibilities, and artifacts required to support functional stakeholder activities. The ICIB members established a process for prioritizing iEHR capabilities in collaboration with the IPO and the technical community that is supported by the IPO Advisory Board. An important part of this effort is the establishment of C-IPTs to analyze each capability and support the requirements definition process. The iEHR C-IPTs bring together subject matter experts (SMEs) from all three Military Departments, TRICARE Management Activity (TMA), and VA to perform business architecture, requirements engineering, and business process re-engineering activities. This approach is the culmination of months of strategic planning to identify a standard process that will guide each capability through the development lifecycle, and will meet the needs of both Departments' functional end users. Products from the C-IPT will help leadership in both Departments assess and select the best EHR IT solution that meets the needs of both Departments.

The ICIB providers, members and staff supported the full C-IPT for the first iEHR clinical capability—Pharmacy—through analysis, decision, documentation, and progression to the completion of an initial Request for Information (RFI) to industry. The Joint Immunization Capability (JIC) began C-IPT activities in September 2011 and is now developing functional requirements and optimizing joint business process models. As an iterative process, these working sessions are building a foundation for the rest of the C-IPT's activities. The staggered

completion of each functional capability's development lifecycle tracks toward the Departments' greater goal of a fully integrated EHR.

b. VA/DoD HEC IM/IT WG

The HEC IM/IT WG is a technical advisory board, composed of technical leaders from the Departments, including Service leaders. It provides oversight of joint integrated health information sharing activities, and ensures that commonly-accepted Government IT program management practices are utilized. The HEC IM/IT WG performs a quality review of architectural artifacts supporting proposed joint functional capabilities and evaluates the technical relevance and feasibility of the proposed joint functional capabilities.

Through the HEC, the IM/IT WG informs the IPO Advisory Board of potential health information sharing issues as they relate to integrated health information sharing initiatives and impact key milestones. This supports efforts of the IPO Director to oversee the development and implementation of DoD/VA integrated health information sharing initiatives.

The IM/IT WG also collaborates on architecture and standards issues with the HARB and works closely with appropriate DoD and VA program offices, which are responsible for development and implementation of applications that will interface or integrate with the iEHR.

As the IPO's new structure matures, the IPO likely will assume many roles and responsibilities now performed by the IM/IT WG; accordingly, the need to continue the IM/IT WG will be reviewed periodically.

c. Health Architecture Review Board (HARB)

The HARB serves as an advisory working group to the HEC. The HARB is a collaborative forum in which the Departments' representatives establish the architectural direction for the development of health IT (HIT) initiatives. To ensure effective coordination on HIT initiatives between the Departments, the HARB addresses the standards, quality assurance, integration, transparency, visibility, and monitoring of EA needed for interagency HIT. The HARB also is

responsible for collaborating with standards development organizations (SDOs)[1] by supporting current efforts, providing comments, and initiating standards development efforts.

The HARB participates in the HEC strategic planning process and recommends initiatives for HIT procurement and/or development of required architecture in support of HIT applications, where appropriate.

The DoD Co-Chair of the HARB is the CTO, TMA. The VA Co-Chair is the Director, EA. The placement of the HARB within the governance structure may change as the IPO's new organization matures.

3. VA/DoD Health Executive Council (HEC)

The HEC—co-chaired by DoD's Assistant Secretary of Defense for Health Affairs (ASD(HA)) and VA's Under Secretary for Health—is the decisional body to which the ICIB, HEC IM/IT WG, HARB, and other WGs report. Within the governance structure for the iEHR, the HEC provides high-level interagency cooperation and coordination in a shared effort to improve healthcare services and reduce healthcare costs for the Departments' beneficiaries.

The HEC is responsible for reviewing plans of each Department for the acquisition of healthcare services and resources. For example, the HEC reviews plans for new facilities and major equipment and technology acquisitions to identify and promote opportunities for coordination and collaborative sharing of healthcare resources. It also establishes and maintains the joint DoD/VA iEHR functional mission statement, measures of performance and effectiveness, key performance parameters, and business process models that enable the IPO Director and IPO Advisory Board to perform their management functions. The HEC reviews the implementation of activities designed to promote the coordination and sharing of health-related services and resources between the Departments, and recommends to the VA/DoD Joint Executive Council (JEC) the strategic direction, policy development, and implementation processes appropriate to support initiatives identified in the JEC Strategic Plan (JSP).

---

[1] The term "standards development organization" means a domestic or international organization that plans, develops, establishes, or coordinates voluntary consensus standards using procedures that incorporate the attributes of openness, balance of interests, due process, an appeals process, and consensus in a manner consistent with the Office of Management and Budget Circular A-119.

4. IPO Advisory Board

For senior-level oversight, the Secretaries of the Departments have designated the DoD Deputy Chief Management Officer (DCMO) and the VA Assistant Secretary (Information and Technology) as the senior officials responsible for overseeing efforts of the IPO. The DoD DCMO and VA Assistant Secretary (Information and Technology) co-chair a newly-chartered IPO Advisory Board, comprising senior leadership of both Departments. The IPO Advisory Board will support actions to:

- Approve program and acquisition plans, resources, and prioritized functional requirements/capabilities, including sequence of clinical capability, common service needs, and gaps to be filled;
- Provide the necessary Milestone Decision Authority responsibility for the iEHR and VLER Health;
- Determine strategic priorities, functional/performance requirements, data standards and compliance, architectural requirements, clinical workflows, business process reengineering, system and infrastructure requirements; and
- Monitor progress toward program milestones including cost, schedule, and performance with regular IPO Director In-progress Reviews.

5. VA/DoD Joint Executive Council (JEC)

Co-chaired by the VA Deputy Secretary and the Under Secretary of Defense (Personnel and Readiness) (USD (P&R)), the JEC is responsible for the strategic direction, policy development, and implementation processes that support initiatives identified in the JSP. In accordance with statute, the JEC institutionalizes the Departments' electronic health information sharing and collaboration to ensure the efficient use of services and resources for the delivery of healthcare and other authorized benefits to Service members, Veterans and beneficiaries.

6. Senior Military Medical Advisory Council (SMMAC)

Tri-Service coordination of health matters, including HIT, occurs through the SMMAC. The SMMAC involves MHS leadership in a deliberative review process for healthcare policy review, implementation and accountability. Key SMACC participants include the Military Departments' Surgeons General and the Principal Deputy Assistant Secretary of Defense (Health Affairs) (PDASD(HA)).

C. Management Foundation for the iEHR Enterprise Architecture

The iEHR EA rests on a strong management foundation within the IPO. The IPO will include a senior Technical Director, a senior Chief Architect, and a senior Director of ED&T. The Chief

Architect and the Director of ED&T will directly matrix staff to support the iEHR and VLER Health PMs. This senior leadership will be critical to ensure that the iEHR and VLER Health are guided by a robust EA. The Chief Architect is primarily responsible for managing the EA program and documentation process, selecting and implementing the EA framework and documentation methodology, identifying EA standards, and managing EA configuration management sub-processes. Other key management stakeholders and their respective roles and responsibilities include:

- **C-IPT Architects**, who participate in EA program decision making, are responsible for identifying IT-related requirements and EA solutions for each C-IPT, capturing knowledge, optimizing business processes, and modeling information;
- **Systems Architects**, who provide technical analysis and design support for systems-related EA component selection and implementation, ensure that IT systems meet migration and interoperability requirements, and support EA documentation;
- **Data Architects**, who provide technical analysis and design support for database-related EA component selection and implementation, ensure that databases meet integration and interoperability requirements, and support EA documentation;
- **SMEs**, who identify end user requirements for EA components on C-IPTs and provide feedback on the effectiveness of solutions; and
- **Requirements Analysts**, who document and verify C-IPT and end user requirements, and assist in EA component design and documentation activities.

Key EA management support personnel include:

- **EA Tool Experts**, who provide software application and database maintenance and support; and
- A **Webmaster**, who is responsible for maintenance of the EA Web site, content development and publishing tools, and links to external Web sites as needed.

D. Development of Initial Versions of the iEHR Enterprise Architecture

The initial versions of the iEHR and VLER Health EA will leverage the EA work previously completed in the Departments. This work is described below.

1. Functional and Technical Assessment of the Electronic Health Record Way Ahead (EHRWA) Enterprise Architecture

In fulfilling a congressional reporting request under section 716 of the NDAA FY 2010, DoD performed an assessment of the capability of the EHRWA EA to achieve optimal clinical

practices and healthcare outcomes, and generated a plan to take any corrective actions necessary to remedy shortfalls identified as a result of this assessment. The resulting assessment and plan were submitted to congressional defense committees in the June 2010 report, *Improvements to the Governance and Execution of Health Information Management and Information Technology Programs*.

A high performance team (HPT)—led by the DoD Deputy Chief Information Officer (DCIO)—conducted a functional and technical assessment of the EHRWA EA. The 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. A functional analysis team, co-chaired by the offices of the DCMO, USD (P&R), and DCIO, assessed whether the EA supports the requirements and gaps identified in the EHR Initial Capabilities Document. A technical analysis team, led by DCIO, assessed whether the proposed solution is consistent with the information EA; utilizes enterprise services; incorporates approved or mandated IT standards; and is consistent with the Department's data and services strategies, information assurance requirements, and radio frequency spectrum policies.

The Department found the EHRWA EA to be sufficient to realize desired capabilities; it also found the EHR technical architecture, although in its early stages, to be consistent with relevant best practices, DoD policy, and IT standards necessary to achieve interoperability. The Government Accountability Office (GAO) was directed by section 716 to assess DoD's compliance with specified reporting requirements, and in its November 2010 report to congressional defense committees, GAO found that DoD had addressed this requirement.

2. Foundation of the iEHR Enterprise Architecture

Development of initial versions of the iEHR EA is underway. The joint DoD/VA functional and technical assessment of the EHRWA EA that preceded iEHR EA development is providing a springboard for current efforts. Now both the foundation of the iEHR EA and the transition plans from the current EA to the target iEHR EA are being established. Underlying components must facilitate interoperability and cost effectiveness, as the increasing cost of maintaining legacy systems continues to be a driver for change.

The Departments have made significant progress with respect to architectural components of the iEHR EA. The EA will continue to mature steadily as the acquisition program progresses through the Departments' acquisition processes. Four illustrations of progress appear in the following discussions of the ESB, DoD Data Model Mapping, Identity Management, and VA consolidation into DISA data centers.

a. Enterprise Service Bus (ESB)

Acquisition of a common ESB and use of a shared CSB approach were among the core iEHR agreements reached by the Departments. On January 13, 2012, a task order was awarded by the

VA Office of Acquisition Operations, Technology Acquisition Center (TAC), to AMS Research, Inc. Subsequently, on February 28, 2012, this award was terminated for convenience of the government. On March 20, 2012, the VA TAC made a new award to Harris Corporation which includes a Sandbox for early developer access and demonstration of product capabilities in the MHS Development and Testing Center (DTC), optimization, testing, regional implementation and sustainment. Next steps include coordination for ESB deployment within operating environment at the MHS DTC with SOA suite demonstration efforts and of hosting of SOA suite Sandbox at the Pacific Joint Information Test Center.

b. DoD Data Model Mapping

To integrate functional content of the iEHR, a common information model will be used by all groups involved in describing the functional capabilities. To facilitate appropriate semantic interoperability among EHR repositories, the Departments have adopted a common information interoperability framework, which includes a common information model, a common terminology model, information exchange specifications, and a translation service. The framework's target architecture is based on use of national standards, such as the Systematized Nomenclature of Medicine Clinical Terminology (SNOMED-CT) and Logical Observation Identifiers Names and Codes (LOINC). The first iteration of the framework, however, will be based on the DoD Data Model. The DoD Data Model uses a translation mechanism that enables the mapping of data sources that adhere to national standards as well as the mapping of data sources that do not adhere to national standards. The latter include the legacy Composite Health Care System (CHCS) and VistA data stores. When necessary, the framework will be extended by the IPO and vendors to support systems analysis, data impacts on CSB development, and data center consolidation efforts supporting the iEHR.

The Departments have agreed to map all VA VistA sites to the DoD Data Model to achieve semantic interoperability and expect to accelerate the mapping of controlled medical vocabulary data for at least one VA VistA site—Salt Lake City. By mapping VA data to the DoD Data Model, the elements will be concretely defined and consistently translated into a single data model that provides interoperability. That single data model will enable the Departments to seamlessly access and aggregate that data into a single logical data store. Use of the interpretation capabilities of a common information interoperability framework will also enable communication with other legacy stores until national standards are incorporated natively.

c. Identity Management

For many years, DoD has viewed identity management as a key tenet of its effort to improve the Department's security posture and achieve efficiencies in the management of digital identities. DoD maintains the following family of products that support individual identification to systems and services in a physical and virtual world.

- **DoD Electronic Data Interchange Person Identifier (EDI PI)—virtual credential**: An EDI PI is provided to all persons whose records exist within DoD's person data repository, the Defense Enrollment Eligibility Reporting System (DEERS). Recipients include DoD civilian, military, retiree, contract support, and family members, DoD beneficiaries, and VA beneficiaries. The EDI PI is a unique number used across DoD as an identifier for DoD systems to manage accounts/records and communicate between systems about individuals without using a social security number. VA has agreed to adopt the EDI PI, allowing information systems in both Departments to access beneficiary records and assign access controls. Joint use of the EDI PI is an essential component for combining data from disparate systems in DoD and VA.

- **DoD Common Access Card (CAC)—physical identification and virtual credential**: A CAC is provided to DoD civilians, DoD military personnel, and selected contract support personnel. The DoD CAC is the Department's Homeland Security Presidential Directive (HSPD) 12 Personal Identity Verification (PIV) credential. The James A. Lovell Federal Health Care Center (JAL FHCC) enabled both DoD CAC access and VA PIV access to the Departments' systems. Future architecture will capitalize on this work for system and data access.

- **Non-CAC DoD identification cards—physical identification**: DoD identification cards are provided to DoD family members, DoD retirees, and DoD beneficiaries to support benefits and entitlements.

- **DoD Self-Service (DS) Logon credential—virtual credential**: A DS Logon is offered to all active/reserve military, military retirees, DoD family members, and VA beneficiaries. It is a simple credential (such as a username and password) that is intended to be used by individuals to view and act on their own information. The credential is linked to an individual's affiliation with DoD/VA, is supported by Federal identity proofing processes, and helps authenticate beneficiaries to DoD, VA, and joint DoD/VA systems. DoD intends to provide DS Logon credentials to all military personnel while they are affiliated with DoD so the credential can transition with them to VA. To date, more than one million DS Logon credentials have been distributed; they are primarily used by the Departments' self-service applications and portals (e.g., TRICARE Online, eBenefits, and milConnect).

DoD envisions many DoD and most joint DoD/VA systems using virtual credentials as a means to authenticate beneficiaries to services (such as patient portal capabilities under the iEHR) and to exchange information among systems. The process to enable systems is ongoing and is expected to occur over several years.

Identity credentials are an important component of the Departments' information systems and will be important to the iEHR. These credentials are used both to ensure that access is provided to the appropriate authorized users and to protect personally identifiable information. Identity credentials are also extendable to provide role-based attributes for user efficiency and effectiveness within systems applications.

Standards-based identity management capabilities are included among the required solutions for the implementation of the Departments' planned iEHR. The IPO is responsible for oversight of this initiative and has met informally with identity management vendors to learn about current industry trends, application, and standards. DoD is leveraging existing identity management services and will continue to seek support, tools, and services from the private sector to improve and align these services.

Identity management efforts are focused on implementation of a common identifier (EDI PI) for DoD/VA patients and on developing attribute-based access for DoD/VA employees. This common identifier will follow an individual for life, as an employee, beneficiary, Veteran, or retiree. DoD is working with VA and third party health providers to promote this identity management scheme to improve the ability to use credentials and provide service to Veterans. The Departments have partnered on a strategy to improve identity management capabilities and the exchange of information within and between DoD/VA systems. The vision has been to establish an individual identity once, and then leverage it and subsequent credentials based on that identity multiple times for various DoD/VA systems.

d. DoD/VA Data Center Consolidation and Cloud Computing

On September 30, 2011, the Departments signed a Memorandum of Agreement underlying their plan to consolidate VA data centers into existing DISA data centers. This cost effectiveness measure aligns with the Federal Data Center Consolidation Initiative (FDCCI). FDCCI was launched in February 2010 and is integral to the *25 Point Implementation Plan to Reform Federal Information Technology Management* issued by the Federal Chief Information Officer on December 9, 2010.

The DoD's approach for consolidation increases reliance on core data centers to support critical enterprise services and reducing component data centers. Core data centers will gradually absorb applications and services hosted in component data centers, allowing these component data centers to be closed. The Data Center and Server Consolidation Reference Architecture, a DoD-wide reference architecture, is being developed to guide data center consolidation and optimization efforts and to achieve Department goals as part of the IT Enterprise Strategy and Roadmap. Key impacts include increased mission effectiveness and security, and achievement of enterprise-wide efficiencies through green IT practices.

Tangible savings—both direct and indirect—are expected to result from consolidation. These savings are expected to be achieved through reduced personnel and infrastructure costs, reduced power and cooling needs, and greater operational efficiency. Improved workload utilization will enable remaining data centers to operate more efficiently. As referenced in the DoD 2011 Data Center Consolidation Plan and Progress Report, most data centers historically operate at a level between 15 and 30 percent and consolidation increases operation to over 65 percent.[2]

Additional reductions that decrease costs include standardization of storage, networks and operating systems, which reduces the complexity of infrastructure. Other opportunities include reductions in real estate holdings, hardware lifecycle replacement costs, software licensing, information assurance, specialized technical and functional application support needs, and monitoring requirements.

Qualitative impacts associated with data center consolidation include:

- **Enhanced Mission Effectiveness**: Consolidation of data centers and servers increases mission effectiveness for the network community and functional users. Opportunities created by consolidation include centralizing management, streamlining operations and standardizing on a more flexible architecture. These changes are beneficial when performing disaster recovery operations and maintenance and when addressing system outages and resource utilization imbalances.

- **Improved Security**: Benefits of data center and server consolidation include improved network, data, and physical security. Opportunities to enhance network security include the use of intrusion detection and prevention systems in centralized data centers. Expedited certification and accreditation processes can be achieved by hosting virtualized servers in pre-configured, standardized hosting enclaves.

- **Streamlined IT Provisioning and Effectiveness**: The development and delivery of new capabilities are expedited through standardized provisioning. Data centers with standardized infrastructures require less effort and resources to operate and maintain. Greater commonality drives interoperability between systems, supports reuse, and drives down costs.

As noted in the DoD 2011 Data Center Consolidation Plan and Progress Report, data center consolidation goals include:

---

[2] DoD 2011 Data Center Consolidation Plan and Progress Report, November 8, 2011.

- Procuring application hosting and IT services from DISA (or commercial sources) which reduce the need for local contractor support and services.
- Hosting and managing applications in DISA Defense Enterprise Computing Centers and/or large contracted commercial computer centers which shifts the focus of IT operations from infrastructure management to a service management model outlined in Federal cloud computing strategy.
- Hosting applications in secure core data centers supports implementation of better standardization, automation and continuous risk monitoring.

The Department is aware of the request in the National Defense Authorization Act, 2012, that the DoD Chief Information Officer develop a plan to use commercial cloud computing services. Analysis of the security, interoperability, and best value implications of this action continues.

3. Transition Planning

a. Transition Application Plan (TAP)

The DoD has embarked on a comprehensive transition planning effort, led by the PEO of JMIS and the CTO. The TAP includes an overall architectural roadmap and a system-by-system plan for transition. DoD continues to mature the TAP to define the expected transition between current and future EHR and component systems' target states. The TAP outlines the methodology to address functionalities of the current EHR and its existing legacy programs, projects, and initiatives. Newly acquired modules and/or applications will consume or replace legacy systems and older functionalities, and older functionalities will be turned off as the transition into the iEHR occurs. The TAP will continue to evolve as the Departments jointly define, acquire, and evolve the iEHR.

The TAP will facilitate and synchronize the technical, functional, infrastructure, and financial management of the process of transitioning clinical and business functionalities to the iEHR EA. The TAP's overarching goal is to assist PMs in planning for the transition of legacy programs, projects, and initiatives (PPI) while maintaining program alignment with the iEHR acquisition schedule as it is developed. The desired end state is an iEHR characterized by a sustainment funding level at or below the legacy sustainment cost baseline. The plan will inform the execution of the FY 2013 President's Budget and FY 2014 Program Objective Memorandum (POM), as well as reviews of the FY 2012 budget.

The TAP and its associated appendices define the expected transition between the current and future EHR and component systems' target states. The plan outlines the methodology to address functionalities of the current EHR and its existing PPI. It leverages existing and previous efforts to identify the best approach to provide continuity of service for each functional capability set, while realigning budgets to sustain planned future capabilities. The TAP supports detailed planning to ensure that: required functionalities, data and business rules are implemented in the

iEHR before turning off legacy functionality; fiscal and infrastructure are synchronized with transition; and training and end user acceptance is complete.

The current draft TAP assumes that all funds/budgets for legacy products will remain associated with those products under the management of MHS HIT program offices through FY 2014. The TAP will be adjusted as needed to reflect senior-level decisions about when specific iEHR capabilities will be implemented. The transition plan reflects those decisions, but does not drive them. Approval of the TAP is expected in November 2012.

b. Transition Planning Methodology and Management

As the iEHR plan matures, the TAP will be continuously updated. Leaving a gap in transition planning is known to be a weakness in IT system implementation. Therefore, as part of the overall iEHR effort, TMA is also establishing a transition office to ensure that required transition activities for DoD EA and legacy systems impacted by the iEHR are well planned and well executed.

Numerous systems of the Departments provide support to clinical and functional community business processes. Accomplishing system migrations in a planned, repeatable manner requires a good understanding of existing systems and of interim and end-state architectures. It is also important to have visibility into the overall enterprise work space to ensure business continuity and collaboration. The transition planning methodology integrates various industry standards and best practices to provide a predictable implementation plan. The methodology elements follow:

- **Understand Legacy Systems**: Understand legacy systems that support the functional community and infrastructure enablers. Collect and document interfaces through which data traverses between legacy systems.

- **Perform Value Analysis**: Perform business value and technology maturity analyses to understand the relative use of systems. This analysis facilitates identification of base costs for upgrades applied to legacy systems, to allow those systems to consume interim iEHR capabilities or transition to the future state.

- **Plan Migration of Interfaces to Services**: As the enterprise moves into SOA, convert most standalone point-to-point information conduits to services that can be created once and reused by others requiring the same services. This action helps ensure a reduction in development and maintenance costs for interfaces.

- **Perform Level of Effort and Costing Analysis**: Based on functional needs, perform required analysis to determine whether to enhance existing systems or replace them with new systems. This action involves estimating the effort required to create the services, the

infrastructure required to host services, and costs for the infrastructure.

- **Generate Transition Plan**: Based on the prioritized capability, generate an implementation plan that allows the eventual implementation of infrastructure, services, and systems. This action will involve synchronizing with portfolio management teams to ensure that tasks are embedded appropriately into current or planned projects.

- **Maintain Transition Plan**: Continuously maintain the transition plan with updates based on implementation and new details in an effort to ensure continuity, reduce uncertainty, and increase confidence in plan execution. This action is a key integrating component through which programs and systems can be measured and prepared for the overall iEHR transition and implementation.

II. Investment

The Departments have adopted business rules for acquiring system capabilities. First, purchase commercially available solutions for joint use. Second, if available, adopt a Department-developed application solution. Third, approve joint application development on a case-by-case basis. Last, obtain IPO Advisory Board review if one Department does not use an application developed by the other.

Capital investment selections for the iEHR EA will be made by the IPO Director. A myriad of factors will impact selection decisions. These include the iEHR EA; interagency cost estimates for the iEHR program; and the technical approach. Other factors include enhanced governance models; the HARB; the EAMP; existing agreements between the Departments about capabilities and common requirements within a common conceptual architecture; and the establishment of functional iEHR capability sets, including technical services. Each of these factors is discussed below.

A. iEHR Enterprise Architecture

The Departments intend the iEHR EA to help guide the process of selecting, developing, transitioning, and integrating HIT investments for the iEHR, by improving program performance, resource planning and allocation, and actions contributing to interoperability.

1. Program Performance

The iEHR EA improves visibility and transparency of investments through the creation of investment dashboards. These dashboards detail sequencing and prioritization plans that are critical to optimizing IM/IT success. The iEHR EA enhances two fundamental EA activities: IT Portfolio Analysis and Investment Review.

2. IT Resource Planning and Allocation

There is a long-term focus on blueprinting inherent trade-offs and resource prioritization among competing interests, initiatives, or programs within the Departments. The iEHR EA places a strong emphasis on the holistic needs and priorities of the Departments; funding investments will not be made based on the needs of individual programs. As iEHR EA content and artifacts evolve, DoD/VA iEHR EA will reflect a sequencing strategy based on enterprise priorities, resources, dependencies, and constraints. The iEHR EA provides awareness to leadership on potentially redundant or overlapping investments. It can be leveraged to assist in eliminating duplicative investments, resulting in reduced system development and operation/maintenance costs. The iEHR EA promotes the sharing of common services and the establishment of enterprise-wide standards. The iEHR EA will synchronize and align efforts described within each Department's EA.

3. Contribution to Interoperability

The iEHR EA will assist the DoD/VA drive towards enterprise-wide standards to promote actions and planning, resulting in greater interoperability across disparate applications and systems, both internally and externally to the organization.

B. Cost Assessment and Program Evaluation (CAPE) Office

In 2011, DoD CAPE, working with VA Office of Corporate Analysis and Evaluation (CA&E), completed an initial review of the existing cost estimate for the iEHR program. Insufficient program definition existed during this review for DoD CAPE and VA CA&E to provide an assessment of the iEHR program cost estimate. The cost estimate will continue to be refined as the program matures. DoD CAPE and VA CA&E review informed the FY 2013 budget submission.

For the upcoming milestone event, the Milestone Decision Authority has directed the program to address risk factors identified by CAPE in its assessment of the Analysis of Alternatives, including a risk mitigation strategy and updated cost estimates. Additionally, DoD CAPE and VA CA&E will develop an interagency cost estimate to support this upcoming milestone event. The DoD CAPE and VA CA&E interagency cost estimate will also include an assessment of alternatives and the associated estimated costs, as directed by the Deputy Secretary of Defense. The results of these analyses and the interagency cost estimate will be used to baseline the program for full system acquisition, to include the required full funding.

C. Technical Approach

In charting its approach to the iEHR EA, the Departments have received technical guidance from a contractor that has found no significant issues with the conceptual target iEHR EA, and recommended specific areas where increased attention to technical underpinnings would support

a successful joint program approach. The Departments will continue to support ongoing technical risk mitigation as the iEHR and VLER Health mature.

D. Governance Model / Charters

The governance model for the iEHR EA is discussed above in Part I.B. Multiple charters were developed or revised to support the iEHR. These structures include a combined requirements generation process leveraging a re-chartered ICIB and HEC IM/IT WG; a new HARB; the existing HEC; a re-chartered and more empowered IPO; and a new IPO Advisory Board. Processes described in new and revised charters are already in use to support iEHR efforts. Senior level oversight is provided by the JEC, and Tri-Service coordination is provided by the SMMAC.

E. Health Architecture Review Board (HARB)

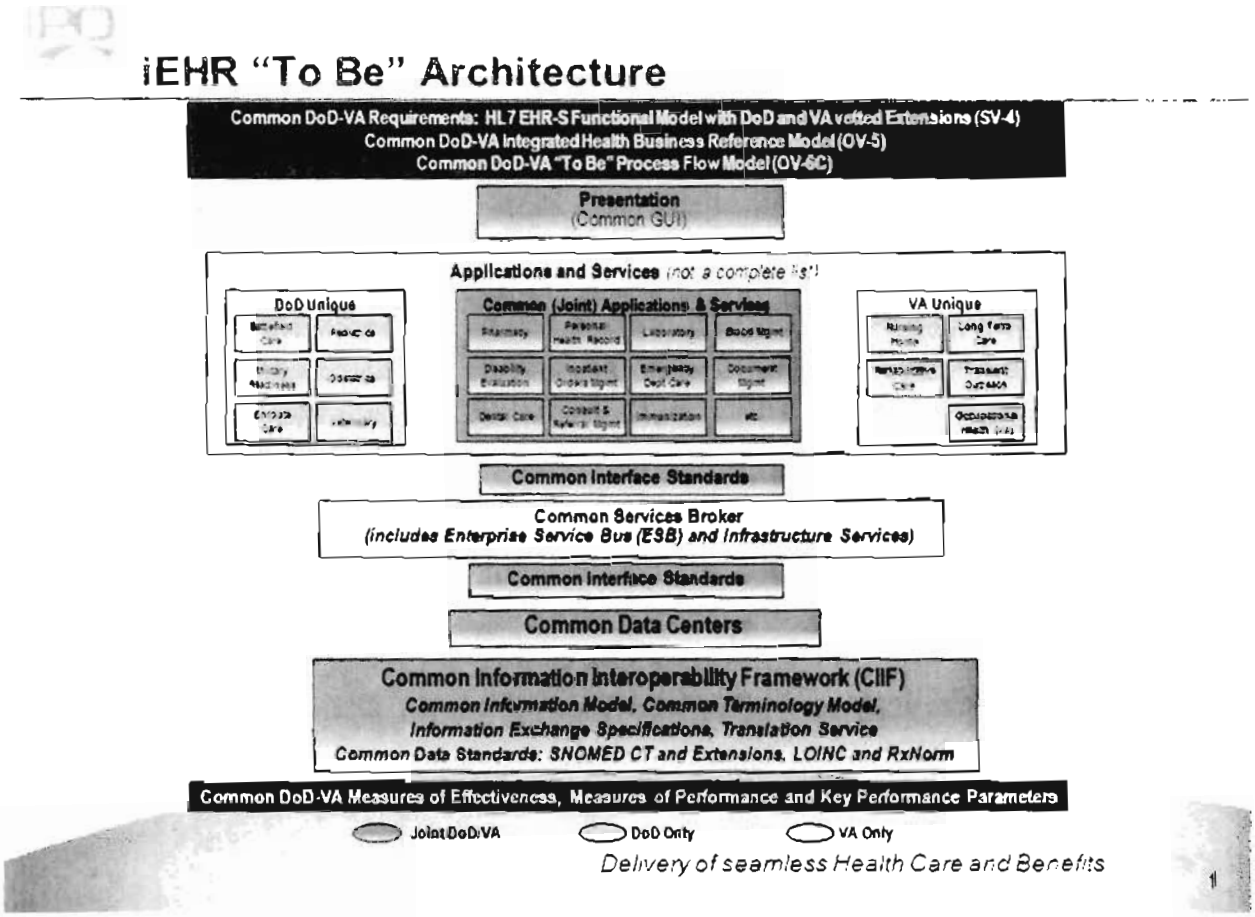
The HARB, discussed in Part I.B.2.c., will help guide development of foundational architecture documentation. The HARB will provide architecture oversight and approval due diligence for joint DoD/VA health programs to facilitate interagency cooperation and foster collaboration on EA for interagency HIT initiatives.

F. Enterprise Architecture Management Plan (EAMP)

The iEHR EAMP, discussed above in Part II, plays an important role in investment selection. The EAMP defines the role of EA within the iEHR, and its associated stakeholders and governance bodies. The EAMP describes the current joint EA, and articulates the process by which future joint architecture products will be developed. It also outlines the iEHR EA program, and its intent to align and unify DoD/VA strategic initiatives, business processes, information flows, systems and services, and technology infrastructure. The intent of the EAMP is to ensure that all major initiatives, processes, projects, IT standards and investments support the stated DoD/VA mission, vision, and strategic goals and objectives.

G. Conceptual Architecture

The Departments are pursuing the iEHR from a position of strength, with agreement on a common conceptual architecture. The following figure sets forth the conceptual architecture; this architecture will continue to evolve as the Departments proceed to develop DoD- and VA-specific capabilities and common requirements. Meeting the Departments' joint and respective functional needs is the essence of the iEHR.



H. iEHR Functional Capability Sets

Functional capabilities of the iEHR are being approached in capability sets. The ICIB, the functional advisory board discussed in Part I.B.2.a, recommends the priorities of capability sets and the sequence of work within them. Each capability in each Capability Set is tracked through a system development and governance lifecycle. This lifecycle begins with a capability queue and continues to development of: (1) a functional business process, (2) high-level functional requirements, (3) a solution review, (4) an acquisition strategy, and (5) program monitoring and control.

The enabling feature capability set will be a threshold accomplishment; it will comprise both

technical and clinical services of the iEHR. Technical services are to include a test environment, core services, and supporting infrastructure, such as the ESB. Clinical services are to include credentialing, orders service, CDS and secure messaging, both provider-to-provider and patient-to-provider.

In constituting early capability sets, the ICIB will define the initial capabilities of the iEHR. Capability Set 1[3] has been separated into subsets A and B, based on the extent of their development within the capability development framework (CDF). The more mature set, Set 1A, currently includes pharmacy (inpatient, outpatient, and inventory management), supporting infrastructure, immunization, and dental care. The nascent set, Set 1B, includes emergency department care, laboratory, personal health record, consult and referral management and care management. Candidates for future Capability Sets have been identified: inpatient documentation, outpatient documentation, anatomic pathology, and disability evaluation.

Technical and architectural analysis of the enabling feature set will continue in the near term. Work to finalize Capability Set 1, define the IOC and timeline, and identify capability leads for Set 1 is also continuing. This systematic approach to the iEHR will support the alignment of enterprise resources and investments with enterprise-wide business needs and programs.

III. Reporting under Section 715 of the Ike Skelton NDAA FY 2011

Section 715 required that DoD report to the congressional defense committees on three topics. Each is addressed below.

A. The Ike Skelton NDAA FY 2011, Section 715(c)

The report under section 715(c), on the status of DoD's implementation of recommendations in the GAO Report, *Information Technology: Opportunities Exist to Improve Management of DoD's Electronic Health Record Initiative*, GAO-11-50, was filed April 20, 2011.

---

[3] The functional capabilities listed here were prioritized by the ICIB and are current as of December 5, 2011.

B. The Ike Skelton NDAA FY 2011, Section 715(b)

The report under section 715(b), *Report to Congressional Defense Committees on Health Information Technology Organizational Structure and Future Plans*, was filed September 23, 2011.

C. The Ike Skelton NDAA FY 2011, Section 715(a)

Section 715(a) required an enterprise risk assessment methodology study of DoD HIT programs. DoD's response follows.

Substantial information and analysis are available in a prior related report to congressional committees, GAO's assessment of that report, and DoD's expanded response to GAO. In the following paragraphs we summarize those prior reports and discuss the foundation and application of the Enterprise Risk Assessment Methodology (ERAM) HIT risk management methodology, including tracking methods. Finally, risk management opportunities are viewed in the context of the developing iEHR EA.

1. Prior Related Reports

In its report dated June 21, 2010, *Improvements to the Governance and Execution of Health Information Management and Information Technology Programs*, DoD responded to a congressional provision substantially similar to the one in section 715(a); namely, that under section 716 of the NDAA FY 2010 to report to the congressional defense committees on improvements to the governance and execution of health IM/IT programs planned and programmed to electronically support MHS clinical medical care. For each health IM/IT program covered by the report, DoD was asked to identify and assess risks associated with achieving timelines and goals of the program and a plan of action to mitigate risks identified. In addition, DoD was asked to submit a plan for taking corrective actions necessary to remedy shortfalls identified as a result of the assessments.

As called for in section 716 of the NDAA FY 2010, GAO reviewed DoD's report and assessed DoD's plan of action to achieve goals and mitigate health IM/IT risks. In GAO's November 2010 report to congressional defense committees, *Health Information Technology: DoD Needs to Provide More Information on Risks to Improve Its Program Management*, GAO 11-148, GAO recommended that DoD report additional details concerning risk identification and assessment, risk mitigation planning, and corrective action planning. On November 9, 2010, after concluding its review of GAO's draft report, DCMO sent a letter of concurrence to GAO's Director of Information Management and Human Capital Issues. The letter appended an enhanced mitigation plan, which included a complete list of risks, risk level definitions, and an assessment of each risk's level. For each risk, the organization responsible for risk mitigation activities was listed and estimated resource needs were provided. GAO acknowledged in its final report that DoD's enhanced plan "showed progress in addressing shortcomings identified in the report."

2. Foundation of Risk Management for Defense Acquisition

To manage risk, MHS HIT program offices follow the fundamental objectives and elements of risk management for defense acquisition as stated in the *Defense Acquisition Guidebook* and the *Risk Management Guide for DoD Acquisition*, Sixth Edition version 1, August 2006. Further, MHS HIT program offices use the Carnegie Mellon Software Engineering Institute's (SEI's) Continuous Risk Management (CRM) approach to managing project risks. CRM is a software engineering practice with processes, methods, and tools for managing risks in a project. It provides a disciplined environment for proactive decision-making and is a key reference cited in the *Risk Management Guide for DoD Acquisition*.

a. Defense Acquisition Guidebook

The following excerpt from *Defense Acquisition Guidebook*, Chapter 4, Section 4.2.3.1.5, discusses risk management:

> **4.2.3.1.5. Risk Management**
>
> Risk management is the overarching process that encompasses identification, analysis, mitigation planning, mitigation plan implementation, and tracking. Risk management should begin at the earliest stages of program planning and continue throughout the total life cycle of the program. Additionally, risk management is effective only if it is fully integrated with the program's systems engineering and program management processes. This is accomplished through the identification of risk drivers, dependencies, root causes, and consequence management. A common misconception, and program office practice, concerning risk management is to identify and track issues (vice risks) and then manage the consequences (vice the root causes). Risks should not be confused with issues (realized risks). If a root cause is described in the past tense, the root cause has already occurred, and is therefore an issue that needs to be resolved but not a risk.
>
> Risk management is critical to acquisition program success. Addressing risk on programs helps ensure that program cost, schedule, and performance objectives are achieved at every stage in the life cycle and communicates to stakeholders the process for uncovering, determining the scope of, and managing program uncertainties. Because risk can be associated with all aspects of a program, it is important to recognize that risk identification is part of everyone's job, not just that of the systems engineer or program manager.
>
> **Risk**: Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints. Risk can be associated with all aspects of a program (e.g., threat environment, hardware, software, human interface, technology maturity, supplier capability,

design maturation, performance against plan) as these aspects relate across the work breakdown structure and Integrated Master Schedule.

The impact of software development and integration efforts should be addressed as part of the program's risk management activities. Risk addresses the potential variation in the planned approach and its expected outcome.

Risk has three components:

- A future root cause (yet to happen), which, if eliminated or corrected, would prevent a potential consequence from occurring,
- A probability (or likelihood) assessed at present of that future root cause occurring, and
- The consequence (or effect) of that future occurrence.

A future root cause is the most basic reason for the presence of a risk. Accordingly, risks should be linked to future root causes and their effects.

The risk management process includes the following key activities, performed on a continuous basis: Risk Identification; Risk Analysis; Risk Mitigation Planning; Risk Mitigation Plan Implementation; and Risk Tracking.

Risk Identification: Risk identification is the activity that examines each element of the program to identify associated root causes, begin their documentation, and set the stage for their successful management. Risk identification begins as early as possible in successful programs and continues throughout the program with regular reviews and analyses of Technical Performance Measurements / Critical Technical Parameters, schedule, resource data, life-cycle cost information, Earned Value Management data/trends, progress against critical path, technical baseline maturity, safety, operational readiness, and other program information available to program Integrated Product Team members.

The intent of risk identification is to answer the question "What can go wrong?" by:

- Looking at current and proposed staffing, process, design, supplier, operational employment, resources, dependencies, etc.,
- Monitoring test results especially test failures (readiness results and readiness problems for the sustainment phase),
- Reviewing potential shortfalls against expectations,

- Analyzing negative trends, and
- Conducting system safety and environmental analyses.

Risk Analysis: The intent of risk analysis is to answer the question "How big is the risk?" by:

- Considering the likelihood of the root cause occurrence;
- Identifying the possible consequences in terms of performance, schedule, and cost; and
- Identifying the risk level using the Risk Reporting Matrix.

Each undesirable event that might affect the success of the program (performance, schedule, and cost) should be identified and assessed as to the likelihood and consequence of occurrence. A standard format for evaluation and reporting of program risk assessment findings facilitates common understanding of program risks at all levels of management. The Risk Reporting Matrix is typically used to determine the level of risks identified within a program. The level of risk for each root cause is reported as low (green), moderate (yellow), or high (red).

Risk Mitigation Planning: The intent of risk mitigation planning is to answer the question "What is the program approach for addressing this potential unfavorable consequence?" One or more of these mitigation options may apply:

- Avoiding risk by eliminating the root cause and/or the consequence,
- Controlling the cause or consequence,
- Transferring the risk, and/or
- Assuming the level of risk and continuing on the current program plan.

Risk mitigation planning is the activity that identifies, evaluates, and selects options to set risk at acceptable levels given program constraints and objectives. Risk mitigation planning is intended to enable program success. It includes the specifics of what should be done, when it should be accomplished, who is responsible, and the funding and schedule tasks required to implement the risk mitigation plan. The most appropriate program approach is selected from the mitigation options listed above and documented in a risk mitigation plan. The level of detail depends on the program life-cycle phase and the nature of the need to be addressed. However, there must be enough detail to allow a general estimate of the effort required and technological capabilities needed based on system complexity.

Risk Mitigation Plan Implementation: The intent of risk mitigation (plan) execution is to ensure successful risk mitigation occurs. It answers the question "How can the planned risk mitigation be implemented?"

It:

- Determines what planning, budget, schedule tasks, requirements and contractual changes are needed,
- Provides a coordination vehicle with management and other stakeholders,
- Directs the teams to execute the defined and approved risk mitigation plans,
- Outlines the risk reporting requirements for on-going monitoring, and
- Documents the change history.

Implementing risk mitigation should also be accomplished by risk category, and it is important for this process to be worked through the integrated product team structure, requiring the integrated product teams at each work breakdown structure level to scrub and endorse the risk mitigations of lower levels. It is important to mitigate risk where possible before passing it up to the next work breakdown structure level. In addition, each integrated product team must communicate potential cost or schedule growth to all levels of management. It is imperative that the Systems Engineer and Program Manager understand and approve the mitigation plan and examine the plan in terms of secondary, unforeseen impacts to other elements of the program outside of the risk owning integrated product team. As part of this effort, the integrated product teams should ensure effective mitigation plans are implemented and ongoing results of the risk management process are formally documented and briefed, as appropriate, during program and technical reviews.

Risk Tracking: The intent of risk tracking is to ensure successful risk mitigation. It answers the question "How are things going?" by:

- Communicating risks to all affected stakeholders,
- Monitoring risk mitigation plans,
- Reviewing regular status updates,
- Displaying risk management dynamics by tracking risk status within the Risk Reporting Matrix, and
- Alerting management as to when risk mitigation plans should be implemented or adjusted.

Risk tracking activities are integral to good program management. At a top level, periodic program management reviews and technical reviews provide much of the information used to identify any performance, schedule, readiness, and cost barriers to meeting program objectives and milestones. Risk tracking documents may include: program metrics, technical reports, earned value reports, watch lists, schedule performance reports, technical review minutes/reports, and critical risk processes reports.

Typical risk sources include:

- **Threat**. The sensitivity of the program to uncertainty in the threat description, the degree to which the system design would have to change if the threat's parameters change, or the vulnerability of the program to foreign intelligence collection efforts (sensitivity to threat countermeasure).

- **Requirements**. The sensitivity of the program to uncertainty in the system description and requirements, excluding those caused by threat uncertainty. Requirements include operational needs, attributes, performance and readiness parameters (including key performance parameters), constraints, technology, design processes, and work breakdown structure elements.

- **Technical Baseline**. The ability of the system configuration to achieve the program's engineering objectives based on the available technology, design tools, design maturity, etc. Program uncertainties and the processes associated with the "ilities" (reliability, supportability, maintainability, etc.) must be considered. The system configuration is an agreed-to description (an approved and released document or a set of documents) of the attributes of a product, at a point in time, which serves as a basis for defining change.

- **Test and Evaluation**. The adequacy and capability of the test and evaluation program to assess attainment of significant performance specifications and determine whether the system is operationally effective, operationally suitable, and interoperable.

- **Modeling and Simulation (M&S)**. The adequacy and capability of M&S to support all life-cycle phases of a program using verified, validated, and accredited models and simulations.

- **Technology**. The degree to which the technology proposed for the program has demonstrated sufficient maturity to be realistically capable of meeting all of the program's objectives.

- **Logistics**. The ability of the system configuration and associated documentation to achieve the program's logistics objectives based on the system design, maintenance concept, support system design, and availability of support data and resources.

- **Production/Facilities**. The ability of the system configuration to achieve the program's production objectives based on the system design, manufacturing processes chosen, and availability of manufacturing resources (repair resources in the sustainment phase).

- **Concurrency**. The sensitivity of the program to uncertainty resulting from the combining or overlapping of life-cycle phases or activities.

- **Industrial Capabilities**. The abilities, experience, resources, and knowledge of the contractors to design, develop, manufacture, and support the system.

- **Cost**. The ability of the system to achieve the program's life-cycle support objectives. This includes the effects of budget and affordability decisions and the effects of inherent errors in the cost estimating technique(s) used (given that the technical requirements were properly defined and taking into account known and unknown program information).

- **Management**. The degree to which program plans and strategies exist and are realistic and consistent. The government's acquisition and support team should be qualified and sufficiently staffed to manage the program.

- **Schedule**. The sufficiency of the time allocated for performing the defined acquisition tasks. This factor includes the effects of programmatic schedule decisions, the inherent errors in schedule estimating, and external physical constraints.

- **External Factors**. The availability of government resources external to the program office that are required to support the program such as facilities, resources, personnel, government furnished equipment, etc.

- **Budget**. The sensitivity of the program to budget variations and reductions and the resultant program turbulence.

- **Earned Value Management System**. The adequacy of the contractor's EVM process and the realism of the integrated baseline for managing the program.

Risk Management Tools: There are many types of software solutions available to help you with risk management tasks. Each tool provides some specific capability as part of an overall Risk Management process. The tools can largely be broken down into the following categories:

- **Risk Management Systems** [are] Web-based, highly scalable systems (running on databases such as MS SQL Server or Oracle) that integrate into planning or requirements applications (such as Telelogic DOORS, MS Project or Primavera) and assist with the identification, assessment, management, analysis, reporting and communication of risk information (cost, schedule, technical, etc.) on projects and operations.

- **Standalone Tools** may be Web-based or client tools that are limited in scalability (normally running on databases such as Excel or Access) that assist with some or all of the following on smaller projects: identification, assessment, analysis, and communication of risk information.

- **Analysis Tools** assist in the quantification of risk information (normally one or more of the following: cost, schedule and/or technical) from either a risk register or a planning applications (such as Microsoft Project or Primavera).

b. **Risk Management Guide for DoD Acquisition**

The *Risk Management Guide for DoD Acquisition* sets forth fundamental methodologies for risk identification, analysis, mitigation planning, mitigation plan implementation, and tracking. DoD encourages PMs to apply the guidance to all acquisition efforts and program elements. DoD further advises PMs to tailor methodologies to suit unique program elements, statutory requirements, and lifecycle phases.

3. **Application of Risk Management Methodologies to HIT Acquisition**

Risk management methodologies specific to DoD HIT acquisition, which are discussed above in section 2.a., are established in accordance with applicable rules and procedures, and tailored to meet unique program elements, statutory requirements, and life-cycle phases. PMs assess risks, establish mitigation plans, and monitor performance of products, services, and initiatives within their purview. The Defense Health Information Management System (DHIMS) program office provides IM/IT solutions that capture, manage, and share healthcare data for the military's EHR. The Defense Health Services Systems (DHSS) program office builds or maintains products in the areas of business intelligence, clinical support, medical logistics, and resources. The MHS Cyberinfrastructure Services (MCiS) program office provides global delivery of flexible and efficient cyberinfrastructure services by identifying and implementing proven advances in

technology. PMs review risk assessment reports for the clinical and non-clinical product, service, and initiative within their purview.

In July 2010, MHS OCIO and PEO JMIS launched a broader effort to manage risk, chartering a Risk Management Community of Practice (RSKM CoP) and charging it with exchanging risk management practices across MHS to support organizational learning. In addition to sharing best practices, RSKM CoP is linking the SEI CRM to DoD's ERAM process and VA's Critical Analysis and Risk Assessment (CARA) methodology, to ensure consistency with Government activities across the healthcare continuum.

An initial cross-mapping of CRM to ERAM was performed in the fourth quarter of FY 2011. A detailed analysis of this initial cross-mapping is ongoing. Its completion is expected by the third quarter of FY 2012. Once mapping is completed, the RSKM CoP will begin linkage with CARA.

4. Risk Assessment under the iEHR Enterprise Architecture

A methodical review of enterprise risk management methodology will be beneficial in connection with development and implementation of the iEHR EA, as DoD looks to a future state that is cost-effective and interoperable. The iEHR EA will facilitate risk assessment, as it formalizes the identification of stakeholders, dependencies, and technical and functional relationships. In the EA's intentional and structured environment, common, recurring risks will be more visible across programs.

IV. DoD/VA Interagency Program Office (IPO)

Prior to the establishment of the iEHR initiative, the IPO was tasked with responsibility for integrating the Departments' program management plans and activities—to include requirements, schedules, costs and performance measures—for joint HIT initiatives, including JAL FHCC, VLER Health, and EHR modernization efforts. The IPO coordinated recurring meetings, hosted a virtual collaboration Web site, and prepared programmatic documentation such as plans and progress reports on the status of joint HIT efforts. Most recently, the IPO has focused on coordinating the development of key VLER Health program management documentation, including a concept of operations and joint strategic plan.

Section 717(a)(4) of the NDAA FY 2012 asks DoD to address "the role of the IPO to manage or oversee efforts with respect to the future electronic health records program." With the commitment of the Secretaries of the Departments to the joint pursuit of HIT modernization activities through the iEHR, the Departments agreed to delegate additional management responsibility to the IPO. To that end, the Departments revised the IPO's charter to incorporate responsibilities for the iEHR and VLER Health oversight and implementation. (The revised IPO charter is attached as Exhibit A.) The Departments are now taking administrative action to ensure that the IPO is properly sized and staffed to meet its management responsibilities. Since

the IPO's responsibilities are supported by statutory authority under the Wounded Warrior Act, the Departments do not propose further legislative action to support the IPO in performing its expanded mission.

V. Conclusion

DoD respectfully submits this report, demonstrating how IT systems, materiel investments, people, and processes are aligned to guide the transition of DoD's EHR to a future state that is cost-effective and interoperable. Together, the Departments are committed to pursuing a joint, common platform enabled through appropriate governance for the iEHR. The Departments have already identified many synergies and common business processes, including common data standards and data center consolidation, common clinical applications, and a common presentation layer. The DoD is pleased to provide this information to the congressional defense committees, and support our mutual commitment to the health and well-being of our Service members and Veterans.

Department of Defense Enterprise Architecture to Guide the Transition of the DoD Electronic Health Record, and Related Matters

Acronyms and Abbreviations

ADM	Acquisition Decision Memorandum
API	application protocol interface
ASD (HA)	Assistant Secretary of Defense (Health Affairs)
BCL	business capability lifecycle
C&A	certification and accreditation
CA&E	Corporate Analysis and Evaluation Office (VA)
CAC	Common Access Card (DoD)
Capability Set	functional capability sets
CAPE	Cost Assessment and Program Evaluation Office (DoD)
CARA	Critical Analysis and Risk Assessment methodology (VA)
CDF	Capability Development Framework
CDS	clinical decision support
CHCS	Composite Health Care System
C-IPT	Capability Integrated Product Team
CRM	Continuous Risk Management
CSB	common service broker
CTO	Chief Technology Officer
DBS	Defense Business Systems
DCIO	Deputy Chief Information Officer
DCMO	Deputy Chief Management Officer
DEERS	Defense Enrollment Eligibility Reporting System
Department	DoD or VA
Departments	DoD and VA
DHIMS	Defense Health Information Management Systems
DHSS	Defense Health Services Systems
DISA	Defense Information Systems Agency
DoD	Department of Defense
DS	DoD Self-Service
DTC	Development and Test Center
EA	enterprise architecture
EAMP	Enterprise Architecture Management Plan
ECCF	Enterprise Conformance and Compliance Framework
ED&T	Engineering, Development & Testing
EDI PI	Electronic Data Interchange Person Identifier

EHR	electronic health record
EHRWA	EHR Way Ahead
ERAM	Enterprise Risk Assessment Methodology (DoD)
ESB	enterprise service bus
FCPG	Functional Capabilities Planning Group
FDCCI	Federal Data Center Consolidation Initiative
Federal	United States federal
FY	fiscal year
GAO	Government Accountability Office
Government	Federal government
HA	Health Affairs
HARB	Health Architecture Review Board
HEC	VA/DoD Health Executive Council
HEC IM/IT WG	HEC IM/IT Workgroup
HIT	health information technology
HPT	high performance team
HSPD	Homeland Security Presidential Directive
ICIB	DoD/VA Interagency Clinical Informatics Board
IDS	intrusion detection system
iEHR	integrated Electronic Health Record
IM	information management
IOC	initial operating capability
IPO	DoD/VA Interagency Program Office
IPS	intrusion protection system
IT	information technology
JAL FHCC	Captain James A. Lovell Federal Health Care Center
JEC	VA/DoD Joint Executive Council
JIC	Joint Immunization Capability
JSP	VA/DoD JEC Strategic Plan
LOINC	Logical Observation Identifiers Names and Code
MCiS	MHS Cyberinfrastructure Services program office
MEHRC	MHS Electronic Health Record Center
MHS	Military Health System
NDAA	National Defense Authorization Act
PDASD	Principal Deputy Assistant Secretary of Defense

PEO	Program Executive Officer
PIV	Personal Identity Verification
PL	Public Law
PM	Program Manager
POM	Project Objective Memorandum
PPI	programs, projects and initiatives
RFI	Request for Information
RSKM CoP	Risk Management Community of Practice
RTEP	Request for Task Execution Plan
SDO	standards development organization
SEI	Carnegie Mellon Software Engineering Institute
Services	military services, unless context clearly indicates otherwise
SME	subject matter expert
SMMAC	Senior Military Medical Advisory Council
SNOMED-CT	Systematized Nomenclature of Medicine Clinical Terminology
SOA	service oriented architecture
SOI	service oriented infrastructure
TAP	Transition Application Plan
TCO	Total Cost of Ownership
TIMPO	TriService Information Management Program Office
TMA	TRICARE Management Activity
USD (P&R)	Under Secretary of Defense (Personnel and Readiness)
VA	Department of Veterans Affairs
VistA	Veterans Information Systems and Technology Architecture
VLER	Virtual Lifetime Electronic Record
VLER Health	VLER health initiative
WG	Workgroup or Work Group

Department of Defense
and
Department of Veterans Affairs
Interagency Program Office (IPO) Charter

I. **Purpose.** The Interagency Program Office for the Department of Defense (DoD) and the Department of Veterans Affairs (VA) (i.e., the Departments):

a. Serves as the single point of accountability for the Departments in the development and implementation of the integrated electronic health record (EHR) and Virtual Lifetime Electronic Record (VLER) Health systems, capabilities, and initiatives with the goal of full interoperability between the DoD and VA.

b. Is authorized by the Departments to lead, oversee, and manage all interagency planning, programming and budgeting, contracting, architecture, capability acquisition and development, data strategy and management, testing and evaluation planning, infrastructure requirements and funding, common services, implementation, and sustainment related to and including the integrated EHR (iEHR) and VLER Health.

c. Serves as the integrated Program Executive Office for iEHR capabilities and systems, and provides direct oversight of all related EHR and VLER Health legacy systems modernization, including open source investments, in the DoD and the VA. The Departments will retain primary focus on sustainment and transition activities.

d. Accelerates the exchange of health care information as well as full interoperability of data for health and benefits between the Departments to support the delivery of health care and benefits.

e. Leads and directs initiatives identified by the IPO Advisory Board, or Department Secretaries/Deputies, and coordinates with the Health Executive Council (HEC) and Benefits Executive Council (BEC) on requirements and business process reengineering, as needed. These initiatives include, but are not limited to, all iEHR capabilities, current and future joint health IT implementations such as the James A. Lovell Federal Health Care Center in North Chicago, IL, and VLER Health.

f. Facilitates the development of and maintains the iEHR Enterprise architecture in conjunction with the efforts of the HEC and its sub-organizations to evolve the current presumptive Departmental EHR architectures into the target iEHR architecture.

g. Establishes implementation plans for iEHR solutions based on compliance with the iEHR enterprise architecture in coordination with recommendations and analysis provided by the HEC and its sub-organizations.

II. Scope.

a. iEHR. With respect to future and existing Departmental capabilities, systems, and budgets associated with the modernization of current EHR systems (e.g., AHLTA, VistA), legacy system interfaces that support or help facilitate health information exchange between the Departments (e.g., Bidirectional Health Information Exchange or Nationwide Health Information Network) and are not specifically part of existing Departmental EHR systems (e.g., included in EHR budgets) are still part of the broader iEHR portfolio, and will be reviewed and approved by the IPO as appropriate. The iEHR portfolio of capabilities and systems is identified in the iEHR Enterprise Architecture.

b. VLER Health. The VLER Health portfolio of capabilities and systems is identified in the VLER Enterprise Architecture.

III. Mission.

a. To lead DoD and VA in the development and implementation of EHR and VLER Health systems, capabilities, and initiatives that allow for full information interoperability between the Departments to better serve service members, Veterans and other eligible beneficiaries.

b. To accelerate the exchange of health care information among the Departments, other federal and private partners, and service members, Veterans, and other eligible beneficiaries.

c. To inform and otherwise complement other information sharing initiatives within DoD and VA to better enable the Departments to proactively provide the full continuum of services and benefits service members and Veterans have earned via veteran/service member centric processes made possible by effective and efficient, standards-based information sharing.

IV. Authority.

a. Statutory Authorities.
   i. The IPO and its associated leadership structure and responsibilities were established in section 1635 of the National Defense Authorization Act (NDAA) for FY 2008, Pub. L. 110-181, as amended by Section 252 of the Duncan Hunter NDAA for FY 2009, Pub. L. 110-417.
   ii. The IPO receives direction, supervision, and control, including project scope definition and execution guidance, from the Department Secretaries and recommendations from the IPO Advisory Board.
   iii. The IPO shall also receive guidance from the Joint Executive Council under section 320 of title 38, United States Code.

b. Derived Authorities from the Departments. To ensure the IPO fulfills its purpose and mission, the Secretary of Defense and the Secretary of Veterans Affairs, respectively, delegate to the Director of the IPO, their authorities to:

i. Acquire, develop, and implement—to include financial management, and information technology (IT) systems acquisition and development—all common DoD-VA EHR and VLER Health systems, capabilities, and initiatives, as defined by the iEHR and VLER enterprise architectures.
ii. In collaboration with the HEC and BEC, collect and integrate the Departments' EHR and VLER Health functional requirements into program roadmap(s)/integrated master schedule.
iii. Develop and propose the interagency budget and acquisition strategies to meet integrated interagency requirements.
iv. Direct the Departments' personnel resources supporting related interagency initiatives.

V. **Reporting Requirements.** Per the NDAA for FY 2008, no later than 1 January each year through 2014, the IPO Director shall submit to the Secretary of Defense, the Secretary of Veterans Affairs, and the appropriate Congressional committees a report on the activities of the IPO for the preceding calendar year.

VI. **IPO Structure.**

a. IPO Director. The IPO Director, whose position was established by the NDAA for FY 2008, will be selected by the Secretary of Defense with concurrence from the Secretary of Veterans Affairs. The IPO Director is also the Program Executive for iEHR and VLER Health and is responsible to:
   i. Acquire, develop, and integrate major joint DoD-VA Health IT capabilities for the iEHR and VLER Health.
   ii. Prescribe the Departments' design, development, integration, evaluation, and deployment strategies for iEHR systems, capabilities, and initiatives.
   iii. Report annually and as otherwise required, to the Secretary of Defense, Secretary of Veterans Affairs, and all relevant Congressional committees on the status of projects, initiatives, and programs under the IPO's purview.

b. IPO Deputy Director. The IPO Deputy Director position, also established by the NDAA for 2008, will be filled by a member of the Senior Executive Service in the Department of Veterans Affairs selected by the Secretary of Veterans Affairs with concurrence from the Secretary of Defense. The IPO Deputy Director is responsible for acting (and authorized to act) in the Director's stead when the Director so designates or is unavailable. The Deputy Director will report to and be under the direction and supervision of the IPO Director. The IPO Deputy Director also serves as the Deputy Program Executive for iEHR and/or VLER Health.

c. The IPO Director will establish a program manager position for iEHR and a program manager position for VLER Health.

d. DoD and VA Department personnel will be assigned or detailed to the IPO to effectively and efficiently meet the purpose and mission of the IPO:
   i. The organization will be staffed by subject matter experts (SMEs) from other VA-DoD efforts (North Chicago, BHIE, Federal Health Information Exchange, Clinical Data Repository/Health Data Repository, etc.), business architecture

SMEs, data and interoperability standards SMEs, functional SMEs (for efforts related to capability requirements) and clinical staff (to address usability and presentation issues). Personnel from the Departments supporting these efforts may be considered assigned or detailed to the IPO for purposes of such efforts.

ii. Personnel working on IPO projects, initiatives, and/or programs will be rated/evaluated by either the IPO Director or the Deputy Director, as appropriate, who will then provide this feedback to the appropriate Department leadership.

iii. The IPO will determine the requirements associated with personnel billets, and, contingent on IPO approval, the DoD and VA will, consistent with Departmental procedures, provide current or potential employees that fulfill these requirements.

iv. The Departments will provide appropriate programmatic support staff sufficient to support task execution.

e. For the purposes of administrative management and supervision, the IPO resides in the TRICARE Management Activity, which is under the authority, direction, and control of the Assistant Secretary of Defense for Health Affairs and the Under Secretary of Defense for Personnel and Readiness, and is subject to the operational oversight of the Deputy Chief Management Officer, in consultation with the Director of the TRICARE Management Activity and the Assistant Secretary for Information Technology, Department of Veterans Affairs.

VII. IPO Responsibilities. The IPO has the following responsibilities:

a. Personnel. The Director, IPO is responsible for:

i. Developing and requesting current and planned personnel requirements in support of initiatives led by the IPO.

ii. Reporting any staff shortages to the Joint Executive Council for any areas that may impact the ability to deliver capabilities on schedule.

iii. Directing, supervising, and evaluating the activities of all personnel within, aligned or detailed to the IPO.

iv. Rating and evaluating personnel in accordance with the performance management systems of their respective Departments.

b. Funding and Financial Management. The Director, IPO is responsible for:

i. Developing interagency initiative and program budget submissions for iEHR, VLER Health and other joint initiatives led by the IPO and will work with the two Departments to support the budgeting requirements for all related IPO activities as required.

ii. Overseeing the expenditure of interagency budgets supporting all IPO work activities.

iii. Approving and overseeing the expenditures of Joint Initiative Funds related to efforts under the IPO's direction.

iv. Assisting the Departments in preparing, briefing and defending budget appropriations required to support interagency initiatives that are under the authority and direction of the IPO.

c. Acquisition/Development. The Director, IPO is responsible for:

i. Serving as the single point of accountability for the Departments for the rapid

development and implementation of all iEHR and VLER Health systems, capabilities, and initiatives.

ii. Developing and executing acquisition strategies, including funding requirements, to meet interagency requirements.

iii. Leading, directing, and managing all interagency capability acquisition and development to include testing and evaluation planning, infrastructure requirements and funding, common services, implementation, and sustainment related to and including the iEHR and VLER Health.

iv. Providing the Departments with all relevant information required to support the DoD's and VA's respective acquisition and contracting processes and policies for those activities referred by the IPO to the Departments.

d. Solution Development and Validation. The Director, IPO is responsible for:

i. In collaboration with the HEC and BEC, collecting and integrating the Departments' EHR and VLER Health functional capability requirements, and defining the interagency set of requirements into program roadmaps and architectures.

ii. Prescribing the technical approach and directing capability development to meet established interagency requirements.

iii. Determining and validating Solution Sets that will meet interagency requirements including integration with Open Source solutions, as applicable.

iv. Developing and executing interagency integration, testing, and implementation strategies, and reviewing Departmental modernization plans for Departmental-specific EHR capabilities and systems to ensure the proposed technical solution will seamlessly integrate to the iEHR and VLER Health solutions.

v. Validating initiative success against interagency integration, testing and implementation strategies.

vi. Exercising final decision authority for reporting initiative status (e.g., success) to the Departments or the IPO Advisory Board.

VIII. Department Responsibilities.

a. Personnel. The Departments are responsible for:

i. Allocating, aligning and/or detailing Departmental personnel in support of initiatives led by the IPO for those functions under the purview of the IPO as agreed to by the Departments.

ii. Fully aligning personnel and activities to IPO-led initiatives, including those for legacy EHR capabilities.

iii. Incorporating ratings and evaluations from the IPO for detailed personnel.

iv. Assisting with recruitment actions to fill vacancies in billets aligned to the IPO.

v. Each Department will provide a second level reviewer for the IPO Director and Deputy Director Performance appraisals.

b. Funding and Financial Management. The Departments are responsible for:

i. Incorporating interagency budget submissions from the IPO into their respective Departmental budgeting processes and cycles as required.

ii. Aligning and expending Departmental funds associated with the interagency budget in accordance with IPO direction while supporting Departmental

financial management processes and controls, including for legacy EHR and VLER Health capabilities. The parties will jointly develop appropriate agreements, including necessary funding mechanisms, to implement the objectives and responsibilities of this charter pursuant to applicable authority.

iii. Leveraging the IPO to prepare, brief and defend Departmental budget appropriations allocated to interagency initiatives under the direction of the IPO.

iv. Planning, programming, budgeting and execution information for related open source efforts and legacy EHR and VLER Health capabilities and adhering to directions provided by the IPO with regard to funding and financial management.

c. Acquisition. The Departments are responsible for:

i. Aligning the IPO-approved interagency acquisition strategies with the respective Departments' acquisition strategies and processes.

ii. Mapping Departmental acquisition milestones to the interagency budget, including for legacy EHR and VLER Health capabilities.

iii. Providing contracting services as required by the IPO for activities supporting IPO acquisition and development activities.

d. Solution Development and Validation. The Departments are responsible for:

i. Establishing the Departments' respective capability requirements, vetting those requirements in joint forums, such as the HEC and BEC, providing those requirements to the IPO, and working with the IPO to develop the iEHR and VLER Health roadmaps.

ii. Identifying and allocating resources to meet interagency goals and initiatives led by the IPO.

iii. Supporting the development and execution of interagency testing strategies.

iv. Incorporating IPO recommendations on Departmental-specific technical solutions for EHR- related capabilities, systems, and initiatives to ensure integration and interoperability with iEHR.

Note: The Director, IPO retains the final decision authority for reporting initiative status (e.g., success) to the Deputy Secretaries and the IPO Advisory Board.

IX. Charter Administration. This charter will become effective upon the later date of the below signatures, and shall be reviewed for applicability at a minimum of every two years, or at the request of the IPO Advisory Board. Modifications of the charter will be made in writing with the written consent of DoD and VA.

X. DoD/VA IPO Advisory Board. The Director, IPO will collaborate with the DoD/VA IPO Advisory Board. The Charter for the DoD/VA IPO Advisory Board is included as an annex to this Charter.

XI. Cancellation. This Charter will be reviewed every two years with modifications presented in writing and the consent of each Department.

Department of Veterans Affairs

By: _____

The Honorable W. Scott Gould

Deputy Secretary of Veterans Affairs

Date 10/27/11

Department of Defense

By: _____

The Honorable William J. Lynn III

Deputy Secretary of Defense

Date 10/05/11

Annex to IPO Charter
DoD/VA IPO Advisory Board Charter

This Agreement between DoD and VA establishes and clarifies the purpose, structure, and responsibilities of the DoD/VA IPO Advisory Board.
Authority: Section 1635 of the National Defense Authorization Act for Fiscal Year 2008 (P.L. 110-181)

I. **Purpose.** Comprised of senior leaders from each organization, the IPO Advisory Board will serve as the primary advisors to the DoD Deputy Chief Management Officer (DCMO) and VA Chief Information Officer (CIO) for all matters related to the iEHR and Virtual Lifetime Electronic Record (VLER) Health initiatives. Additionally, the Board will collaborate with the IPO regarding the overall execution of the program and serve as an advocate for iEHR and VLER Health requirements, workflow, and business functional architecture established by the Health Executive Council (HEC).

II. **Scope of Responsibilities.**

a. Provides advice on overall program execution and performance.

b. Advises the DoD DCMO and VA CIO on the functional and business requirements of iEHR and VLER Health initiatives.

c. Serves as primary advocate for iEHR and VLER Health requirements and workflow established by the HEC.

d. Members of the IPO Advisory Board provide advice and counsel to the DoD DCMO and VA CIO to support their execution of the following responsibilities:
   i. Approving program and acquisition plans, resources, and prioritized functional requirements/capabilities to include sequence of clinical capability, common service needs, and gaps to be filled.
   ii. Providing the necessary Milestone Decision Authority responsibility for the iEHR and VLER Health.
   iii. Determining strategic priorities, functional/performance requirements, data standards and compliance, architectural requirements, clinical workflows, business process reengineering, system and infrastructure requirements in the event of conflict between the HEC and the IPO Director.
   iv. Monitoring progress toward program milestones including cost, schedule, and performance with regular IPO Director In-progress Reviews (IPRs).

III. **Structure.**

a. Chairmanship: The DoD/VA IPO Advisory Board is co-chaired by the DoD DCMO and the VA CIO.

b. Membership:

i. DoD: Deputy Chief Management Officer; Assistant Secretary of Defense (Health Affairs); Joint Staff Surgeon; Chief Information Officer; Director, Operational Test and Evaluation; Director, Cost Assessment and Program Evaluation; Comptroller; Principal Deputy Under Secretary of Defense (Personnel and Readiness); Deputy Assistant Secretary of Defense for Wounded Warrior Care and Transition Policy.

ii. VA: Chief Information Officer; Under Secretary for Health; Under Secretary for Benefits; Chief Technology Officer; Principal Deputy Assistant Secretary for Information and Technology; Principal Deputy Under Secretary for Health; Deputy Under Secretary for Health (Policy and Services); Chief Financial Officer; Assistant Secretary for Policy and Planning.

IV. Procedural Guidelines.

a. Meetings:

i. Meetings are led by the co-chairs and are held every other month. The co-chairs may call additional meetings as required.

ii. IPO Advisory Board recommendations are made by mutual consensus of the co-chairs utilizing inputs from the Advisory Board members and supporting working groups as the basis for their recommendations.

b. Administration: The DoD DCMO, in consultation with the VA CIO, shall appoint an Executive Secretary to the DoD/VA IPO Advisory Board to monitor assignments, disseminate recommendations, coordinate sub-council and work group activities, and provide other support as required.

c. Review of Charter: This charter will be reviewed annually from the date of approval. Dissolution of the DoD/VA IPO Advisory Board or modifications to this charter will be made in writing and will become effective upon the written concurrence of the DoD DCMO and the VA CIO.

V. Reporting. The DoD/VA IPO Advisory Board reports to the DoD DCMO and the VA CIO.

SEC. 717. LIMITATION ON AVAILABILITY OF FUNDS FOR THE FUTURE ELECTRONIC HEALTH RECORDS PROGRAM.

(a) LIMITATION.—Of the funds authorized to be appropriated by this Act or otherwise made available for fiscal year 2012 for the procurement, research, development, test, and evaluation, or operation and maintenance of the future electronic health records program, not more than 10 percent may be obligated or expended until the date that is 30 days after the date on which the Secretary of Defense submits to the congressional defense committees a report addressing—

(1) an architecture to guide the transition of the electronic health records of the Department of Defense to a future state that is cost-effective and interoperable;

(2) the process for selecting investments in information technology that support the architecture described in paragraph (1);

(3) the report required by section 715 of the Ike Skelton National Defense Authorization Act for Fiscal Year 2011 (Public Law 111–383; 124 Stat. 4249);

(4) the role of the Interagency Program Office to manage or oversee efforts with respect to the future electronic health records program; and

(5) any other matters the Secretary considers appropriate.

(b) FUTURE ELECTRONIC HEALTH RECORDS PROGRAM DEFINED.—In this section, the term ''future electronic health records program'' means the programs of the Department of Defense referred to as the ''EHR way ahead'' and the ''virtual lifetime electronic record''.

111TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

HASC No.
5

IKE SKELTON NATIONAL DEFENSE AUTHORIZATION ACT FOR FISCAL YEAR 2011

COMMITTEE PRINT

OF THE

COMMITTEE ON ARMED SERVICES HOUSE OF REPRESENTATIVES

LEGISLATIVE TEXT AND
JOINT EXPLANATORY STATEMENT

TO ACCOMPANY

H.R. 6523

PUBLIC LAW 111–383

DECEMBER 2010

the congressional defense committees a report on the findings of the review under paragraph (1).

(b) ANNUAL REPORT ON GRADUATE MEDICAL EDUCATION PROGRAMS.—

(1) ANNUAL REPORT.—Not later than April 1, 2011, and annually thereafter through 2015, the Secretary of Defense shall submit to the congressional defense committees a report on the status of the graduate medical education programs of the Department of Defense.

(2) ELEMENTS.—Each report under paragraph (1) shall include the following:

(A) An identification of each graduate medical education program of the Department of Defense in effect during the previous fiscal year, including for each such program, the military department responsible, the location, the medical specialty, the period of training required, and the number of students by year.

(B) The status of each program referred to in subparagraph (A), including, for each such program, an identification of the fiscal year in which the last action was taken with respect to each of the following:

(i) Initial accreditation.

(ii) Continued accreditation.

(iii) If applicable, probation, and the reasons for probationary status.

(iv) If applicable, withheld or withdrawn accreditation, and the reasons for such action.

(C) A discussion of trends in the graduate medical education programs of the Department.

(D) A discussion of challenges faced by such programs, and a description and assessment of strategies and plans to address such challenges.

(E) Such other matters as the Secretary considers appropriate.

SEC. 715. HEALTH INFORMATION TECHNOLOGY.

(a) ENTERPRISE RISK ASSESSMENT METHODOLOGY STUDY.—

(1) STUDY REQUIRED.—The Secretary of Defense shall conduct an enterprise risk assessment methodology study of all health information technology programs of the Department of Defense.

(2) REPORT.—Not later than 180 days after the date of the enactment of this Act, the Secretary shall submit to the congressional defense committees a report containing the results of the study required under paragraph (1).

(b) REPORT ON HEALTH INFORMATION TECHNOLOGY ORGANIZATIONAL STRUCTURE AND FUTURE PLANS.—

(1) REPORT REQUIRED.—Not later than 180 days after the date of the enactment of this Act, the Secretary of Defense shall submit to the congressional defense committees a report on the organizational structure for health information technology within the Department of Defense.

(2) ELEMENTS.—The report required under paragraph (1) shall include the following:

(A) Organizational charts for all organizations involved with health information technology showing, at a minimum, the senior positions in each office and each activity.

(B) A description of the functions and responsibilities, to include policy formulation, policy and program execution, and program oversight, of each senior position for health information technology.

(C) An assessment of how well the health information systems of the Department of Defense interact with the health information systems of—

(i) the Department of Veterans Affairs; and

(ii) entities other than the Federal Government.

(D) A description of the role played by the Interagency Program Office established by section 1635 of the Wounded Warrior Act (title XVI of Public Law 110–181; 10 U.S.C. 1071 note) and whether the office is satisfactorily performing the functions required by such section, as well as recommendations for administrative or legislative action as the Secretary considers appropriate.

(E) A complete description of all future plans for legacy systems and new electronic health record initiatives, including the joint virtual lifetime electronic record.

(F) The results of the survey described in paragraph (3).

(3) SURVEY.—The Secretary shall conduct a survey of users of the health information technology systems of the Department of Defense to assess the benefits and failings of such systems.

(4) DEFINITIONS.—In this subsection:

(A) The term "senior position" means a position filled by a member of the senior executive service, a position on the Executive Schedule established pursuant to title 5, United States Code, or a position filled by a general or flag officer.

(B) The term "senior personnel" means personnel who are members of the senior executive service, who fill a position listed on the Executive Schedule established pursuant to title 5, United States Code, or who are general or flag officers.

(c) REPORT ON GAO REPORT REQUIRED.—Not later than March 31, 2011, the Secretary of Defense shall submit to the congressional defense committees a report on the report by the Comptroller General of the United States titled "Information Technology: Opportunities Exist to Improve Management of DOD's Electronic Health Record Initiative" (GAO–11–50), including—

(1) the status of implementing the recommendations made in such report; and

(2) for each such recommendation that has not been implemented, the reason why the recommendation has not been implemented.

SEC. 716. EDUCATION AND TRAINING ON USE OF PHARMACEUTICALS IN REHABILITATION PROGRAMS FOR WOUNDED WARRIORS.

(a) EDUCATION AND TRAINING REQUIRED.—The Secretary of Defense shall develop and implement training, available through the Internet or other means, on the use of pharmaceuticals in rehabili-

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

Accountability * Integrity * Reliability

GAO-11-148