

June 10, 2005



Information Technology Management

Reporting of DoD Capital Investments for
Information Technology in Support of the
FY 2006 Budget Submission
(D-2005-083)

Department of Defense
Office of Inspector General

Quality

Integrity

Accountability

Report Documentation Page				Form Approved OMB No. 0704-0188	
Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.					
1. REPORT DATE 10 JUN 2005		2. REPORT TYPE N/A		3. DATES COVERED -	
4. TITLE AND SUBTITLE Information Technology Management: Reporting of DoD Capital Investments for Information Technology in Support of the FY 2006 Budget Submission				5a. CONTRACT NUMBER	
				5b. GRANT NUMBER	
				5c. PROGRAM ELEMENT NUMBER	
6. AUTHOR(S)				5d. PROJECT NUMBER	
				5e. TASK NUMBER	
				5f. WORK UNIT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) United States Department of Defense Office of Inspector General 400 Army Navy Drive (801) Arlington, VA 22202				8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)				10. SPONSOR/MONITOR'S ACRONYM(S)	
				11. SPONSOR/MONITOR'S REPORT NUMBER(S)	
12. DISTRIBUTION/AVAILABILITY STATEMENT Approved for public release, distribution unlimited					
13. SUPPLEMENTARY NOTES					
14. ABSTRACT					
15. SUBJECT TERMS					
16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT UU	18. NUMBER OF PAGES 35	19a. NAME OF RESPONSIBLE PERSON
a. REPORT unclassified	b. ABSTRACT unclassified	c. THIS PAGE unclassified			

Additional Copies

To obtain additional copies of this report, visit the Web site of the Department of Defense Inspector General at <http://www.dodig.mil/audit/reports> or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Department of Defense Inspector General
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

DEPARTMENT OF DEFENSE

hotline

To report fraud, waste, mismanagement, and abuse of authority.

Send written complaints to: Defense Hotline, The Pentagon, Washington, DC 20301-1900
Phone: 800.424.9098 e-mail: hotline@dodig.osd.mil www.dodig.mil/hotline

Acronyms

ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
DBSMC	Defense Business Systems Management Committee
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIR	Capital Investment Report
IT	Information Technology
OMB	Office of Management and Budget



INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

June 10, 2005

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE ACQUISITION,
TECHNOLOGY, AND LOGISTICS
UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF
FINANCIAL OFFICER
UNDER SECRETARY OF DEFENSE PERSONNEL AND
READINESS
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND
INFORMATION INTEGRATION /DOD CHIEF INFORMATION
OFFICER

SUBJECT: Report on Reporting of DoD Capital Investments for Information Technology in
Support of the FY 2006 Budget Submission (Report No. D-2005-083)

We are providing this report for review and comment. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. As a result of management comments, we revised Recommendation 1. to clarify our position on improving the quality of information technology reporting to the Office of Management and Budget and Congress, and redirected Recommendation 1. to the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Under Secretary of Defense for Personnel and Readiness, in addition to the Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer. Therefore, we request that the Under Secretary of Defense for Acquisition, Technology, and Logistics and the Under Secretary of Defense for Personnel and Readiness, in addition to the Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer provide comments on revised Recommendation 1. by July 8, 2005.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Audam@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Mr. Robert R. Johnson at (703) 604-9024 (DSN 664-9024). See Appendix E for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Mary L. Ugone
Assistant Inspector General
for Acquisition and Technology Management

Department of Defense Office of Inspector General

Report No. D-2005-083

June 10, 2005

(Project No. D2005-D000AL-0036.000)

Reporting of DoD Capital Investments for Information Technology in Support of the FY 2006 Budget Submission

Executive Summary

Who Should Read This Report and Why? DoD managers preparing and certifying capital investment justifications for information technology should read this report to improve the quality of data being submitted by the Department of Defense to the Office of Management and Budget and Congress.

Background. Information technology is a President's Management Agenda priority for expanding electronic government. In addition, Congress has challenged, in committee report language, the quality of DoD information technology management because information technology documents and associated budget data that DoD provided were inaccurate, misleading, or incomplete. For FY 2006, the DoD Budget Estimate Submission totaled \$30 billion for information technology.

Results. DoD Components did not adequately report information technology investments to the Office of Management and Budget in support of the DoD Budget Request for FY 2006 because Component Chief Information Officers and Chief Financial Officers did not always include required information in submitted reports. Specifically, 157 of 171 (92 percent) Capital Investment Reports submitted to the Office of Management and Budget in September 2004 did not completely respond to one or more required data elements addressing security funding, certification and accreditation, training and security plans, and enterprise architecture. As a result, the quality of DoD information reported to the Office of Management and Budget continues to have limited value and does not demonstrate, in accordance with Office of Management and Budget and DoD guidance, that DoD was effectively managing its proposed information technology investment for FY 2006. See the Finding section of the report for the detailed recommendations.

Management Comments and Audit Response. The Deputy Comptroller, responding for the Under Secretary of Defense(Comptroller)/Chief Financial Officer, commented that responsibility for review and compilation of information technology (IT) material, primarily the IT-43 exhibits, was realigned from the Under Secretary of Defense (Comptroller) to the Office of the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) on January 14, 1998, and the Under Secretary of Defense (Comptroller) organization that was responsible for the IT-43 exhibits has been disestablished. We agree that a 1998 realignment occurred; however, the Congress and the Deputy Secretary of Defense have recently directed that the Under Secretary of Defense (Comptroller)/Chief Financial Officer; the Under Secretary of Defense for Personnel and Readiness; and the Under Secretary of Defense for Acquisition, Technology, and Logistics assume specific responsibilities with regard to information

technology governance, in addition to those responsibilities assigned to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (see Appendix D). Recommendation 1. has been revised and redirected to reflect this guidance.

The Deputy Assistant Secretary of Defense (Resources), responding on behalf of the Acting Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, partially concurred and commented that the concurrent DoD/Office of Management and Budget program and budget review process rendered it neither feasible nor logical to withhold submission of Component information technology budget requests that do not comply with the Office of Management and Budget and congressional requirements, and/or have not been certified by the Component Chief Information Officer and Chief Financial Officer as compliant with the requirements of the DoD Regulation 7000.14-R, "Financial Management Regulation," Volume 2B, Chapter 18, "Information Technology Resources and National Security Systems," June 2004. The Deputy Assistant Secretary of Defense (Resources) commented that she would enlist the help of the Office of the Under Secretary of Defense (Comptroller)/Chief Information Officer to enforce the DoD Financial Management Regulation. As indicated above, Recommendation 1. was revised in light of management comments and recent direction from the Congress and the Deputy Secretary of Defense. See the Finding section of the report for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

We request that the Assistant Secretary of Defense for Networks and Integration/DoD Chief Information Officer; the Under Secretary of Defense (Comptroller)/Chief Financial Officer; the Under Secretary of Defense for Personnel and Readiness; and the Under Secretary of Defense for Acquisition, Technology, and Logistics provide comments on the final report by July 8, 2005.

Table of Contents

Executive Summary	i
Background	1
Objectives	2
Finding	
Completeness of DoD Capital Investment Reports	3
Appendixes	
A. Scope and Methodology	14
Prior Coverage	14
B. FY 2006 Statement of Compliance Submissions by DoD Components	16
C. Exhibit 300 Questions Reviewed	17
D. Recent Information Technology Guidance	19
E. Report Distribution	21
Management Comments	
Under Secretary of Defense (Comptroller)/Chief Financial Officer	23
Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer	25

Background

DoD Components use information technology (IT) in a wide variety of mission functions including finance, personnel management, computing and communication infrastructure, logistics, intelligence, and command and control. Information technology consists of any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, movement, control, display, switching, interchange, transmission, or reception of data or information. The President's Management Agenda for expanding electronic government identified effective planning for information technology investments as a priority. Improving information technology security is one of the Office of Management and Budget's (OMB) highest priorities in information technology management. In addition, Congress has challenged, in committee report language, the quality of DoD information technology management because information technology documents and associated budget data that DoD provided were inaccurate, misleading, or incomplete. The Assistant Secretary of Defense for Networks and Information Integration (ASD[NII]), as the Chief Information Officer (CIO), is the principal staff assistant to the Secretary of Defense for DoD information technology.

Public Law 107-347, Title III, "Federal Information Security Management Act of 2002," December 17, 2002, requires agencies to address the adequacy and effectiveness of information security policies and practices in plans and reports relating to annual agency budgets.

Public Law 104-106, "National Defense Authorization Act for Fiscal Year 1996," Division E, "Information Technology Management Reform," February 10, 1996, commonly called the "Clinger-Cohen Act," requires effective and efficient capital planning processes for selecting, managing, and evaluating the results of all major investments in information technology. The Act requires that executive agencies:

- Establish goals for improving the efficiency and effectiveness of agency operations through the use of information technology;
- Prepare an annual report, to be included in the executive agency's budget submission to Congress, on the progress in achieving the goals;
- Prescribe performance measurements for information technology and measure how well information technology supports agency programs;
- Measure quantitatively agency process performance for cost, speed, productivity, and quality against comparable processes and organizations in the private and public sectors where they exist;
- Analyze the missions of the executive agency and, based on the analysis, revise the executive agency's mission-related processes and administrative processes as appropriate before making significant investments in information technology; and

-
- Ensure that information security policies, procedures, and practices of the executive agency are adequate.

DoD uses the Information Technology Management Application database to plan, coordinate, and disseminate the DoD information technology budget exhibits that OMB and Congress require. The information technology budget request for FY 2006 totaled \$30 billion.

Components must submit an Exhibit 300, “Capital Investment Report,” for all major information technology investments. Major information technology investments:

- require special management attention because of their importance to an agency’s mission;
- were included in the FY 2005 submission and are ongoing;
- are for financial management and more than \$500,000;
- are directly tied to the top two layers of the Federal Enterprise Architecture;
- have significant program or policy implications;
- have high executive visibility; and
- are defined as major investments by the agency’s capital planning and investment control process.

DoD management and OMB use the Exhibit 300 Investment Report to show that the Component has employed the disciplines of good project management, presented a strong business case for the investment, and defined the proposed costs, schedule, and performance goals for the investment if funding approval is obtained. When submitted, the Capital Investment Report (CIR) should be complete and accurate and provide all the information that the Office of Management and Budget requires. In September 2004, DoD submitted 171 CIRs for the FY 2006 budget request to the Office of Management and Budget.

Objectives

The overall audit objective was to assess whether the Services and DoD Components are accurately reporting information technology investment data to the Office of Management and Budget. Specifically, the audit determined whether DoD Capital Investment Reports, that were submitted in September 2004 for the Office of Management and Budget FY 2006 reporting requirements demonstrated that DoD is managing its information technology investments in accordance with the Office of Management and Budget and DoD guidance. See Appendix A for discussion of the scope and methodology.

Completeness of DoD Capital Investment Reports

DoD Components did not adequately report information technology investment data to the Office of Management and Budget in support of the DoD Budget Request for FY 2006 because Component Chief Information Officers and Chief Financial Officers did not always include the required information in the reports that they submitted. Specifically, 157 of the 171 (92 percent) Capital Investment Reports submitted to the Office of Management and Budget in September 2004 did not completely address one or more required data elements in the sections on security and privacy and enterprise architecture compliance. In addition, 47 percent of DoD Components did not provide the required statement of compliance in support of their Capital Investment Report submissions. As a result, the quality of DoD information reported had limited value and did not demonstrate that DoD was effectively managing its proposed \$30 billion information technology investment for FY 2006.

Criteria

Office of Management and Budget Circular A-11. Office of Management and Budget Circular A-11, "Preparation, Submission, and Execution of the Budget," Part 7, section 300, "Planning, Budgeting, Acquisition, and Management of Capital Assets," July 2004, implements the Clinger-Cohen Act and establishes policy and procedures for planning, budgeting, acquiring, and managing Federal capital assets. Agencies are required to demonstrate to OMB in semi-annual reports that major IT investments are directly connected to agencies' strategic plans and provide a positive return on investment, sound acquisition planning, comprehensive risk mitigation and management planning, realistic cost and schedule goals, and measurable performance benefits. For the DoD FY 2006 budget request, the ASD(NII)/DoD CIO forwarded 171 CIRs to OMB. The CIR is the primary means of justifying and managing IT investments.

DoD Financial Management Regulation. The DoD Financial Management Regulation, Volume 2B, Chapter 18, "Information Technology Resources and National Security Systems," June 2004, requires all DoD Components that have any resource obligations for information technology or national security systems to prepare Capital Investment Reports, which are mandated by Circular A-11. The regulation requires Component Chief Information Officers and Chief Financial Officers to jointly attest that the CIRs submitted are complete, accurate, and consistent with the requirements of the Clinger-Cohen Act, Circular A-11, and documented exceptions to the Circular, the DoD CIO budget guidance memorandum, the Paperwork Reduction Act, and other applicable acts and requirements.

National Defense Authorization Act for Fiscal Year 2005. The Ronald W. Reagan National Defense Authorization Act for FY 2005, section 332, "Defense Business Enterprise Architecture, System Accountability, and Conditions for

Obligation of Funds for Defense Business System Modernization,” subsection (h), “Budget Information,” establishes policy and procedures for the Secretary of Defense to follow when submitting budget information to Congress. For FY 2006 and beyond, the Secretary of Defense must identify each DoD business system for which funding is proposed in that budget; identify all funds, by appropriation, proposed in that budget for each system; identify the official to whom authority for each system is delegated; and describe each certification for each system.

Capital Investment Reports to the Office of Management and Budget

The information technology Capital Investment Reports budget request that DoD submitted for FY 2006 did not demonstrate that DoD was effectively and efficiently managing information technology resources in accordance with Circular A-11, July 2004. Our analysis of 171 CIR reports showed that 157 (92 percent) contained incomplete information in one or more sections when compared to criteria in Circular A-11. Information addressing security and privacy and enterprise architecture was missing or incomplete.

Security Funding. Circular A-11 requires DoD Components to describe how security is provided and funded and to report the total dollars allocated for IT security for all FY 2006 investments. Circular A-11 also requires Components to indicate whether an increase in IT security funding is requested to remediate IT security weaknesses, and to specify the amount and a general description of the weakness. Fifty-four of 171 CIR submissions (32 percent) were incomplete. Thirty-two submissions contained requests for FY 2005 security funding instead of the required FY 2006 funding. Six Components did not provide a security funding amount and we were unable to determine the amount of security funding requested for four investments based on the information given. One additional Component specified a security funding dollar amount, but stated, “I am not sure where the dollar amount came from.” In addition, 13 Components did not state how security was provided and funded for their investments and 4 Components provided incomplete information on whether an increase in IT security funding is required to remediate security weaknesses. Table 1 summarizes DoD Components CIRs incomplete security funding information responses for FY 2006 and for FY 2005.

Table 1. Incomplete Submissions for Security Funding		
<u>DoD Component</u>	Percent Incomplete	
	<u>FY 2006</u>	<u>FY 2005¹</u>
Army	19	55
Navy	39	19
Air Force	36	8
Defense agencies	38	28
¹ As reported in DoD IG Report No. D-2005-002, "Reporting of DoD Capital Investments for Technology in Support of the FY 2005 Budget Submission," October 12, 1004		

Certification and Accreditation. Circular A-11 requires DoD Components to verify full certification and accreditation of IT for which investments are made, specify the methodology used, and provide the date of the last certification and accreditation review. Full certification and accreditation refers to the authority to operate and excludes interim authority to operate. All IT for which investments are made must be fully certified and accredited before becoming operational. Anything less than full certification and accreditation indicates that identified IT security weaknesses remain. These weaknesses must be corrected before funding for the investment can be justified. Fifty of 171 (29 percent) investments reviewed were not fully certified and accredited or gave incomplete answers. Inadequate responses included investments with interim authority to operate, no date of last review, no statement of compliance with the DoD Information Technology Security Certification and Accreditation Process, or whether authority to operate had been granted. Components stated that certification and accreditation approval was pending. One stated that it was in the planning phase and that certification and accreditation approval was not required, though the IT investment was in the full acquisition phase. Table 2 summarizes DoD Components CIRs incomplete or noncompliant certification and accreditation responses for FY 2006 and for FY 2005.

Table 2. Incomplete Certification and Accreditation Submissions		
<u>DoD Component</u>	Percent Incomplete	
	<u>FY 2006</u>	<u>FY 2005¹</u>
Army	33	50
Navy	12	56
Air Force	27	33
Defense agencies	36	33
¹ As reported in DoD IG Report No. D-2005-002.		

Incident Handling and Reporting. Circular A-11 requires Components to report on how they incorporated incident-handling capability into the system or information technology investment and to include a summary of intrusion detection monitoring and a review of audit logs. Circular A-11 also requires Components to report on incidents that are reported to the Department of Homeland Security Federal Computer Incident Response Center. Sixty-seven of 171 (39 percent) Capital Investment Reports did not contain the required information for this area. Sixty-two CIRs failed to address all three elements of this question. One Component responded that it did not need to address this area. Some Components stated that their systems were still in development and did not address the question, and other Components stated that incident handling would be incorporated into the system in the future.

Security Plans. Circular A-11 requires Components to report whether information technology investments have an up-to-date security plan and to provide the date and other details of the plan. A simple reference to security plans or other documents is not an acceptable response as stipulated in Circular A-11. Twenty-eight of 171 (16 percent) investments reviewed did not answer those questions adequately or did not confirm that they had a security plan. Components did not always provide information supporting the existence of a security plan or plan dates.

Contractor Security. Circular A-11 requires Components to report whether a contractor operated the system on-site or at a contractor facility and whether the contract includes specific security requirements required by law and policy. Circular A-11 also requires Components to describe how contractor security procedures are monitored, verified, and validated. Twenty-seven of 171 (16 percent) CIRs did not completely address all elements for this area. Other Component responses stated that the IT investment was not a system, and therefore did not include a response. The majority of the investments contained partial responses.

Security Testing. Circular A-11 requires Components to report whether management, operational, and technical security controls were tested for effectiveness and when the most recent tests were performed. Twenty-two of 171 (13 percent) CIRs reviewed did not contain the required information to adequately respond to this question. Some Components failed to confirm whether controls were tested and others did not provide dates.

Security Training. Circular A-11 requires DoD Components to report whether all system users were appropriately trained in the past year, including rules of behavior and consequences for violating those rules. Twenty-one of 171 (12 percent) CIRs did not contain the necessary information to complete this question.

- Responses for 11 investments did not verify training for system users.
- Responses for 3 investments were unclear or provided no answer.
- Responses for 7 investment said that the investment was not a system or that the investment was in development.

Table 3 summarizes the incomplete submissions for the security questions for FY 2006 and for FY 2005.

Table 3. Incomplete Submissions for Security Questions		
Question	Percent Incomplete	
	FY 2006	FY 2005 ¹
Security Plans	17	8
Contractor Security	16	6
Security Testing	13	6
Security Training	12	3

¹As reported in DoD IG Report No. D-2005-002.

Protection of Systems with Public Access. Circular A-11 requires Components to report how agencies use security controls and authentication tools to protect privacy of systems that promote or permit public access. Component responses for this element were highly compliant; only 2 of 171 (1 percent) CIRs were incomplete.

Proper Handling of Personal Information. Circular A-11 requires agencies to handle personal information consistent with relevant Government-wide and agency policies. Component responses for this element were highly compliant; only 5 of 171 (3 percent) CIRs were incomplete.

Federal Information Security Management Act. The Federal Information Security Management Act requires agencies to integrate IT security into their capital planning and enterprise architecture processes, to conduct annual IT security reviews of all programs and systems, and to report the results of those reviews to OMB. In August 2004, the Director, OMB stated in a memorandum that all agency systems must be reviewed annually. Circular A-11 requires Components to report whether they reviewed investments as part of the FY 2004 Federal Information Security Management Act reporting process, whether the review indicated any weaknesses, and whether the weaknesses were included in a corrective action plan. One hundred and eleven of 171 (65 percent) CIRs responded that the investment was reviewed as a part of the FY 2004 Federal Information Security Management Act review process. Of those 110 investments that were reviewed, 14 (13 percent) reported that weaknesses had been found and that the weaknesses were included in a corrective action plan. Sixty of 171 investments (35 percent) reported that they were not reviewed as part of the 2004 Federal Information Security Management Act review process. We found abnormalities in four CIRs. The Navy, the Air Force, and the Defense Finance and Accounting Service submitted investment reports stating that no weaknesses were found during the 2004 Federal Information Security Management Act review process; however, the reports did state that weaknesses were included in a corrective action plan. Table 4 summarizes the percentage of investments reviewed under the Federal Information Security Management Act review process

and the percentage of investments with stated weaknesses that were included in their corrective actions plans for FY 2006 and for FY 2005.

Table 4. Federal Information Security Management Act Review Process

	<u>FY 2006</u>	<u>FY 2005¹</u>
Percent Reviewed Under FY 2004 Act	64	48
Percent of Weaknesses Identified and Included in a Corrective Action Plan	13	13

¹As reported in DoD IG Report No. D-2005-002.

Enterprise Architecture Identification. The Federal Enterprise Architecture is a business and performance-based framework developed to facilitate Government-wide organization and collaboration efforts, so that all Government agencies are efficiently working toward the same goal of serving the public. Agencies submit information on the planning, acquisition, management, and use of IT investments to OMB in the Circular A-11 Exhibit 300s. This information assists OMB in making budget decisions and determining whether the agency practice is consistent with OMB policies and guidance. Each agency should map the IT investments to the reference models for Federal Enterprise Architecture which can identify potential opportunities to collaborate with other Federal agencies and eliminate redundant spending. Circular A-11 requires Components to report whether the investment is identified in the agency's enterprise architecture, and provide an explanation if the investment is not identified. All 171 (100 percent) CIR submissions stated that the investment was identified in their agency's enterprise architecture.

Modernization Blueprint. Circular A-11 requires Components to report whether the IT investment is consistent with the agency 'to be' modernization blueprint. The Exhibit 300 must demonstrate either that the existing investment is meeting the needs of the agency and the expected performance, or that the investment is being modernized and replaced consistent with the modernization blueprint. Four of 171 (2.3 percent) CIRs did not completely address the required information for this area. Two of the IT investments were legacy enterprise systems that will be discontinued.

Enterprise Architecture Review Committee. Circular A-11 requires Components to report whether the IT investment was approved through the agency's Enterprise Architecture Review Committee. Five of 171 (3 percent) CIRs were not approved through their agency's Enterprise Architecture Review Committee.

Process Simplification, Reengineering, and Design Projects. Circular A-11 requires Components to report what major process simplification, reengineering, and design projects are required as part of their IT investment. Eighteen of 171 (11 percent) CIRs did not completely provide information on the projects that were required as part of their IT investment. Nine of the investments failed to

address all areas of the question. Five IT investments reported being exempt from redesigning because they were weapon systems. Two IT investments claimed that major process simplification, reengineering, and design projects did not apply to National Security Systems. Other IT investment reports contained non-responsive answers, or did not respond to the question.

Organization Restructuring, Training, and Change Management Projects.

Circular A-11 requires Components to report what major organization restructuring, training, and change management projects are required. Eleven of 171 (6 percent) CIRs did not provide the required information.

Federal Enterprise Architecture Reference Models. The Federal Enterprise Architecture is based on five reference models that identify duplicate investments, gaps in processes, and opportunities for collaboration through a cross analysis of all Federal agencies. This collaboration can then provide a common structure for all agencies to improve their lines of business, such as budget allocation, information sharing, and performance measurement.

Circular A-11 requires Components to provide information on three models, the Business Reference Model, Service Component Reference Model, and Technical Reference Model. The Business Reference Model describes the mission and purpose of the Federal Government through an organized, hierarchical structured format of the day-to-day business operations. The Service Component Reference Model is a framework that identifies how the Federal Government's service Components, such as process automation, back office support technology, and analytical services support business performance objectives and IT investments and assets. The Technical Reference Model provides a Component-based framework identifying standards, specifications, and technology used to construct and deliver service Component capabilities throughout the Federal Government. Collectively, these reference models establish a foundation to identify, design, and distribute service Components in IT investments across the Federal Government to yield the most efficient means of serving the public.

Lines of Business and Subfunctions. Circular A-11 requires Components to list all the lines of business and subfunctions from the Federal Enterprise Architecture Business Reference Model that the IT investment supports. All 171 investments provided this list in a complete format.

Applications, Components, and Technology. Circular A-11 requires Components to discuss the major investments in relationship to the Service Component Reference Model section of the Federal Enterprise Architecture, including a discussion of the Components included in the major IT investment. Forty-two of 171 (25 percent) CIRs did not complete the table provided to determine how the investment related to the Service Component Reference Model section of the Federal Enterprise Architecture. Circular A-11 also requires Components to state whether all hardware, applications, components, and web technology requirements for the IT investment are included in the Agency Enterprise Architecture Technical Reference Model. Eight of the 171 (5 percent) did not answer the question completely.

Circular A-11 requires Components to discuss the major IT investment in relationship to the Technical Reference Model section of the Federal Enterprise Architecture, identifying each service area, service category, service standard, and service specification that collectively describes the technology supporting the major IT investment. Seventy-three of the 171 (43 percent) CIRs did not complete the table provided to determine their relationship to the Technical Reference Model section of the Federal Enterprise Architecture.

Circular A-11 requires Federal agencies to state whether the application will leverage existing technology components or applications across the Government. Fourteen of the 171 (8 percent) CIRs did not completely answer this question.

Circular A-11 requires financial management systems and projects to be mapped to the agency's financial management system inventory that they provide annually to OMB, identifying the system name(s) and system acronym(s) as reported in the most recent systems inventory update. Ten of the 171 (5 percent) IT investments did not provide the appropriate information on whether the investment's Financial Management System was mapped to the agency's financial management system inventory.

Statement of Compliance Requirement. Forty-seven percent of DoD Components did not provide the required statement of compliance when submitting their Capital Investment Reports in support of the FY 2006 DoD Budget Estimate Submission. In June 2004, DoD revised DoD Financial Management Regulation, Volume 2B, "Budget Formulation and Presentation," to require DoD Component Chief Information Officers and Chief Financial Officers to sign a joint or coordinated transmittal memorandum stating that IT submissions are complete; accurately aligned with primary budget, program and acquisition materials; and are consistent with the requirements of Circular A-11.

The Financial Management Regulation states that statements of compliance must be submitted within 10 calendar days of the submission due date for electronic program and budget submission in September and within 10 calendar days after the Five Year Defense Plan has "locked" for the final IT submission for the President's Budget. Component IT budget submissions are entered into the Information Management Technology Application database administered by ASD(NII) and submitted to OMB for the DoD Budget Estimate Submission and to Congress for the President's Budget. Component IT CIRs not accompanied by a statement of compliance convey uncertainty about their completeness and accuracy as well that of the Information Management Technology Application database used to identify and justify the DoD IT budget request to OMB and Congress. Submission of Component IT investment reports to OMB in support of the DoD Budget Estimate Submission should be postponed until Component statements of compliance are submitted to ASD(NII). Appendix B identifies the status of DoD Components for the FY 2006 statement of compliance. Appendix C identifies the Exhibit 300 questions we reviewed.

DoD Self-Assessment of Component Submissions. On July 19, 2004, the ASD(NII)/DoD CIO issued policy and guidance for completing and submitting the FY 2006 CIRs. Starting with the FY 2006 Exhibit 300 submissions, the Director of Resources, Office of the ASD(NII)/DoD CIO was required to score all

investment report submissions using the newly established internal DoD self-assessment process.

Office of Management and Budget Watch List. The OMB watch list is used to assess the potential risks that a particular IT investment poses. The assessment may determine that additional funding is not suitable for that investment. The OMB has a set of criteria to score 10 different areas of the Capital Investment Reports, based on a score of one to five, five being the highest. The individual scores are then added to form a raw score for the Business Case. If any investment receives a score lower than four for security and privacy, the investment is placed on the OMB watch list. An investment is also placed on the watch list if the overall raw score for the Business Case is below 31.

OMB placed 41 (24 percent) DoD FY 2006 initiatives on the OMB FY 2006 watch list. OMB assigned 22 investments with failing scores for security; the DoD self-assessment also scored 17 of the same 22 investments with failing scores. DoD and OMB assigned passing scores to the same eight watch list investments for security. OMB assigned security passing scores to an additional 11 initiatives, which DoD scored as failing. Six of the 11 DoD-scored initiatives, received scores of two and below. Greater coordination between DoD and OMB on scoring criteria would benefit the CIR evaluation process. Self-assessment time constraints prevented Components from revising deficient initiatives before submitting them to OMB in September 2004.

Conclusion

The quality of DoD information reported on Security and Privacy and Enterprise Architecture to OMB had limited value because it did not demonstrate, in accordance with OMB and DoD guidance, that DoD was effectively managing its requested \$30 billion IT investment for FY 2006. Although reasonable explanations existed for some missing and incomplete data, that rationale could not be applied systemically for the majority of missing or incomplete information responses.

Although CIRs are officially submitted to OMB twice yearly, Components should use them as management tools and update the reports as the information becomes available. Information reported in CIRs help management ensure that spending on capital assets directly supports an agency's mission and will provide a return on investment equal to or better than alternative uses of funding.

Submission of incomplete reports jeopardizes appropriate funding and diminishes the overall usefulness of CIRs. The quality of the data collected is of particular concern because DoD plans to use data collected for Exhibit 300 purposes to respond to other congressional information requests, such as those contained in the National Defense Authorization Act for FY 2005.

Recommendations, Management Comments and Audit Response

Revised Recommendation. As a result of management comments, and in light of recent congressional and Deputy Secretary guidance concerning IT governance (Appendix D), we revised Recommendation 1. to clarify our position on improving the quality of IT reporting to OMB and Congress.

1. We recommend that the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Personnel and Readiness, the Under Secretary of Defense (Comptroller)/Chief Financial Officer, and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer specify the processes that will be followed to ensure that funds are not obligated to DoD information technology and National Security System investments for which the Office of Management and Budget requires a Form 300 Exhibit that are not supported by complete and correct Capital Investment Reports and accompanying signed statements of compliance from the Component Chief Information Officers and Chief Financial Officers, as required by DoD Regulation 7000.14-R, “Financial Management Regulation.”

Management Comments. The Deputy Comptroller, responding for the Under Secretary of Defense (Comptroller)/CFO, commented that responsibility for review and compilation of information technology material, primarily the IT-43 exhibits, was realigned from the Under Secretary of Defense (Comptroller) to the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on January 14, 1998, and the Under Secretary of Defense (Comptroller) organization that was responsible for the IT-43 exhibits has been disestablished. The Deputy Assistant Secretary of Defense (Resources), responding on behalf of the Acting Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, partially concurred and commented that the concurrent DoD/OMB program and budget review process rendered it neither feasible nor logical to withhold submission of Component information technology budget requests that do not comply with OMB and congressional requirements, and/or have not been certified by the Component CIO and CFO as compliant with the requirements of the DoD Regulation 7000.14-R, volume 2B, chapter 18. The Deputy Assistant Secretary of Defense (Resources) commented she would enlist the help of the Office of the Under Secretary of Defense (Comptroller) to enforce DoD Regulation 7000.14-R.

Audit Response. We agree that a 1998 realignment occurred; however, the Congress and the Deputy Secretary of Defense have recently directed that the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense for Personnel and Readiness; and the Under Secretary of Defense (Comptroller)/Chief Financial Office assume specific responsibilities with regard to information technology governance, in addition to those responsibilities assigned to the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (see Appendix D). We request that the Under Secretary of Defense for Acquisition, Technology, and Logistics, the Under Secretary of Defense for Personnel and Readiness, the Under

Secretary of Defense (Comptroller)/Chief Information Officer, and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer provide comments on the final report.

2. We recommend that the Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer improve the quality of information technology reporting to the Office of Management and Budget and Congress by expanding the self-assessment process to include more time for DoD Components to revise deficient investments before making the initial submission to the Office of Management and Budget.

Management Comments. The Deputy Comptroller, responding for the Under Secretary of Defense (Comptroller)/CFO, commented that responsibility for review and compilation of information technology material, primarily the IT-43 exhibits, was realigned from the Under Secretary of Defense (Comptroller) to the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) on January 14, 1998, and the Under Secretary of Defense (Comptroller) organization that was responsible for the IT-43 exhibits has been disestablished. The Deputy Assistant Secretary of Defense (Resources), responding on behalf of the Acting ASD(NII)/DoD CIO, concurred with the recommendation and stated that she would provide time to revise the CIRs and the FY 2007 Budget Estimate Submission.

Audit Response. The Deputy Assistant Secretary of Defense (Resources) comments are responsive to the recommendation and no further comments are requested.

Management Comments to Appendix B. The Deputy Assistant Secretary of Defense (Resources), responding for the Acting ASD(NII)/DoD CIO stated that Appendix B was incorrect because it did not identify all the organizations required to provide statements of compliance. In addition, the American Forces Information Service, the Defense Contract Management Agency, the Defense Logistics Agency, and TRICARE Management Agency did in fact provide statements.

Audit Response. DoD Regulation 7000.14-R requires that statements of compliance be provided within 10 calendar days of the due date of the electronic submission of the program/budget submission in September. Appendix B reflects copies of statement of compliance we received during the verification phase of this audit. Additional statements of compliance were provided after issuance of the draft report on March 29, 2005. Appendix B reflects only the Components required to prepare a FY 2006 CIR.

Appendix A. Scope and Methodology

We examined all 171 CIRs that DoD submitted to OMB for the FY 2006 DoD Budget Request. We limited our review to evaluating responses in the data elements of security funding, certification and accreditation, incident handling and reporting, security plans, contractor security, security testing, security training, protecting systems accessible to the public, and handling private information. We also reviewed the responses in the data elements pertaining to enterprise architecture.

We reviewed DoD Component responses on whether they reviewed IT investments during the FY 2004 Federal Information Security Management Act reporting process. We evaluated the reporting process and the completeness of information for report elements, based on report preparation guidance from Circular A-11 and DoD Regulation 7000.14-R. We did not validate information submitted by DoD Components in the CIRs.

We also reviewed relevant documents pertaining to report submissions dating from December 2002 through May 2005. We met with the analyst responsible for IT budget reports within ASD(NII) to gain an overall understanding of the FY 2006 IT budget process. We reviewed the results of the initial DoD self-assessment of IT budget submissions for FY 2006.

We performed this audit from October 2004 through May 2005 in accordance with generally accepted government auditing standards. We did not review the management control program because it was reviewed in DoD Inspector General Report No. D-2005-023, "Assessment of DoD Plan of Action and Milestones Process," December 13, 2004 and addressed in DoD Inspector General Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005.

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit.

Government Accountability Office High-Risk Area. The Government Accountability Office has identified several high-risk areas in DoD. This report provides coverage of DoD IT Management.

Prior Coverage

During the last 5 years, the Government Accountability Office and the Department of Defense Inspector General have issued five reports discussing the reliability of DoD IT budget submission. Unrestricted Government Accountability Office reports can be accessed over the Internet at <http://www.gao.gov>. Unrestricted DoD Inspector General reports can be accessed at <http://www.dodig.mil/audit/reports>.

GAO

GAO Report No. GAO-04-115, "Improvements Needed in the Reliability of Defense Budget Submissions," December 19, 2003

Department of Defense Office of Inspector General (DoD IG)

DoD Inspector General Report No. D-2005-029, "Management of Information Technology Resources Within DoD," January 27, 2005

DoD Inspector General Report No. D-2005-023, "Assessment of DoD Plan of Action and Milestones Process," December 13, 2004

DoD Inspector General Report No. D-2005-002, "Reporting of DoD Capital Investments for Technology in Support of the FY 2005 Budget Submission," October 12, 2004

DoD Inspector General Report No. D-2004-081, "Reporting of DoD Capital Investments for Information Technology," May 7, 2004

Appendix B. FY 2006 Statement of Compliance Submissions by DoD Components

<u>DoD Component</u>	<u>Submitted a Statement of Compliance for Budget Estimate Submission</u>	
Navy		No
TRICARE Management Agency		No
Defense Logistics Agency		No
Defense Commissary Agency		No
American Forces Information Service		No
Defense Contract Management Agency		No
Defense Information Systems Agency		No
Army	Yes	
Air Force	Yes	
Defense Human Resource Activity	Yes	
Missile Defense Agency	Yes	
Defense Finance Accounting Service	Yes	
U.S. Transportation Command	Yes	
Office of Secretary of Defense	Yes	
Washington Headquarters Services	Yes	
Total	8	7

Appendix C. Exhibit 300 Questions Reviewed

Part I:

d. Was this project reviewed as part of the FY 2004 Federal Information Security Management Act review process?

d.1. If yes, were any weaknesses found?

d.2. Have the weaknesses been incorporated into the agency's corrective action plans?

Part II:

II.A. Enterprise Architecture

A. Is this project identified in your agency's enterprise architecture? If not, why?

A.1. Will this investment be consistent with your agency's "to be" modernization blueprint?

B. Was this investment approved through the EA review committee at your agency?

C. What are the major process simplification/reengineering/design projects that are required as part of this Information Technology investment?

D. What are the major organization restructuring, training, and change management projects that are required?

E. Please list all the Lines of Business and Sub-Functions from the FEA Business Reference Model that this Information Technology investment supports.

II.A.3. Applications, Components, and Technology

A. Discuss this major investment in relationship to the Service Component Reference Model Section of the FEA.

B. Are all of the hardware, applications, components, and web technology requirements for this investment included in the Agency EA Technical Reference Model? If not, please explain.

C. Discuss this major Information Technology investment in relationship to the Technical Reference Model section of the FEA.

D. Will the application leverage existing components and/or applications across the Government (i.e., FirstGov, Pay.Gov, etc)? If so, please describe.

E. Financial Management Systems and Projects, as indicated in Part One, must be mapped to the agency's financial management system inventory provided

annually to the Office of Management and Budget. Please identify the system name(s) and system acronym(s) as reported in the most recent systems inventory update required by Circular A-11 section 52.4.

II.B. Security and Privacy

II.B.1. How is security provided and funded for this investment (e.g., by program office or by the CIO through the general support system/network)?

A. What is the total dollar amount allocated to Information Technology security for this investment in FY 2006? Please indicate whether an increase in Information Technology security funding is requested to remediate Information Technology security weaknesses, specifying the amount and a general description of the weakness.

II.B.2. Please describe how the investment (system/application) meets the following security requirements of the Federal Information Security Management Act, Office of Management and Budget policy, and NIST guidelines:

A. Does the investment (system/application) have an up-to-date security plan that meets the requirements of OMB policy and NIST guidelines? What is the date of the plan?

B. Has the investment been certified and accredited?

C. Have the management, operational, and technical security controls been tested for effectiveness? When were the most recent tests performed?

D. Have all system users been appropriately trained in the past year, including rules of behavior and consequences for violating the rules?

E. Has incident handling capability been incorporated into the system or investment, including intrusion detection monitoring and audit log reviews? Are incidents reported to DHS' FedCIRC?

F. Is the system operated by contractors either on-site or at a contractor facility? If yes, does any such contract include specific security requirements required by law and policy? How are contractor security procedures monitored, verified, and validated by the agency?

Appendix D. Recent Information Technology Guidance

1. Public Law 108-375, Section 332, “Ronald W. Reagan National Defense Authorization Act for Fiscal Year 2005.” Section 2222 requires the Secretary of Defense to delegate responsibility for review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance, and modernization of defense business systems to the:

- Under Secretary of Defense for Acquisition, Technology, and Logistics for any defense business system the primary purpose of which is to support acquisition activities, logistics activities, or installations and environment activities of the Department of Defense;
- Under Secretary of Defense (Comptroller) for any defense business system the primary purpose of which is to support financial management activities or strategic planning and budgeting activities of the Department of Defense;
- Under Secretary of Defense for Personnel and Readiness for any defense business system the primary purpose of which is to support human resource management activities of the Department of Defense; and
- Assistant Secretary of Defense for Networks and Information Integration and the Chief Information Officer of the Department of Defense for any defense business system the primary purpose of which is to support information technology infrastructure or information assurance activities of the Department of Defense National Defense Authorization Act 2005.

2. Deputy Secretary of Defense Memorandum, “Department of Defense (DoD) Business Transformation,” February 7, 2005:

- Establishes the Defense Business Systems Management Committee (DBSMC) mandated by Public Law 108-375;
- Charges the DBSMC with responsibility for ensuring that funds are obligated for Defense Business Systems Modernization in accordance with section 332 of Public Law 108-375; and
- Directs that the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); the Under Secretary of Defense for Personnel and Readiness and ASD(NII)/DoD CIO serve as members of the DBSMC.

3. Deputy Secretary of Defense Memorandum, “Delegation of Authority and Direction to Establish an Investment Review Process for Defense Business Systems,” March 19, 2005:

- Delegates authorities to the Under Secretary of Defense for Acquisition, Technology, and Logistics; the Under Secretary of Defense (Comptroller); the Under Secretary of Defense for Personnel and Readiness and ASD(NII)/DoD CIO for review, approval, and oversight of the planning, design, acquisition, deployment, operation, maintenance, and modernization of defense business systems as required by 10 U.S.C. Section 2222(f); and
- Retains authority with the Deputy Secretary of Defense for any defense business system the primary purpose of which is to support any DoD activity not covered by the above delegations.

4. Deputy Secretary of Defense Memorandum, “Implementation Guidance on the Realignment of the Department of Defense (DoD) Business Transformation Program Management Office,” March 24, 2005, transfers program management, oversight and support responsibilities regarding DoD business transformation efforts from the Office of the Under Secretary of Defense (Comptroller) to the Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics.

5. DoD Directive 5144.1, “Assistant Secretary of Defense Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO),” May 2, 2005, requires that the ASD(NII)/DoD CIO, among other duties, review and provide recommendations to the Secretary and the Heads of the DoD Components on:

- The performance of the Department’s IT and NSS programs (to include monitoring and evaluating the performance of IT and NSS programs on the basis of all applicable performances);
- DoD budget requests for IT and National Security System pursuant to section 2223 of Title 10, U.S.C.;
- The continuation, modification, or termination of an IT and/or National Security System programs or project pursuant to section 1425 of Title 40, U.S.C.; and
- The continuation, modification, or termination of an NII or CIO program pursuant to the Federal Information Security Management Act of 2002 as part of Public Law 107-347, Executive Order 13011, and other applicable authorities.

6. “DoD Investment Review Process Overview and Concept of Operations for Investment Review Boards,” May 11, 2005, establishes the OSD Investment Reviews and will leverage OMB Exhibit 300 reports as well as existing Major Automated Information System processes.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense for Networks and Information Integration/Chief
Information Officer
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Chief Information Officer, Department of the Army
Auditor General, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Financial Management and Comptroller)
Chief Information Officer, Department of the Navy
Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)
Chief Information Officer, Department of the Air Force
Auditor General, Department of the Air Force

Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Under Secretary of Defense (Comptroller)/Chief Financial Officer Comments



COMPTROLLER
(Program/Budget)

OFFICE OF THE UNDER SECRETARY OF DEFENSE
1100 DEFENSE PENTAGON
WASHINGTON, DC 20301-1100

APR 8 2005

MEMORANDUM FOR INSPECTOR GENERAL
(ATTN: DEPUTY INSPECTOR GENERAL FOR AUDITING)

SUBJECT: Reporting of Department of Defense(DoD) Capital Investment for
Information Technology in Support of the Fiscal Year (FY) 2006 Budget
Submission (Project No. D2005AL-0036)

I appreciate the opportunity to review and comment on the Inspector General's draft report on the reporting of DoD capital investment for Information Technology (IT) in support of the FY 2006 budget submission.

The report includes a recommendation that the Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks Information Integration (ASD(NII)) improve the quality of information technology reporting to the Office of Management and Budget and the Congress. On January 14, 1998, the responsibility for review and compilation of information technology material, primarily the IT-43 exhibits, was realigned from Under Secretary of Defense (Comptroller) to the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (ASD(C4I)) (copy attached). As a result of this realignment, the ASD(NII) (formerly ASD(C4I)) issues and maintains the guidance for information technology programs. The Under Secretary of Defense (Comptroller) organization (Information Technology Financial Management Directorate) that was responsible for the IT-43 exhibits has been disestablished.

A handwritten signature in black ink, appearing to read "John P. Roth".

John P. Roth
Deputy Comptroller

Attachment:
As stated

cc: ASD(NII)



OFFICE OF THE SECRETARY OF DEFENSE
WASHINGTON, DC 20301

JAN 14 1998



MEMORANDUM FOR ASSISTANT SECRETARIES OF THE MILITARY DEPARTMENTS
(FINANCIAL MANAGEMENT AND COMPTROLLER)
COMPTROLLERS OF THE DEFENSE AGENCIES
CHIEF INFORMATION OFFICERS OF THE MILITARY
DEPARTMENTS AND DEFENSE AGENCIES

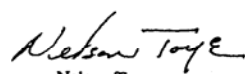
SUBJECT: Transfer of Responsibility for Information Technology Budget Review

As a result of a reorganization in the Office of the Deputy Chief Financial Officer, the Information Technology Financial Management Directorate has been disestablished. Responsibility for review and compilation of information technology budget justification material, primarily the IT-43 Exhibit, has been transferred to the Office of the Deputy Assistant Secretary of Defense for Plans and Resources, under the Office of the Assistant Secretary of Defense (Command, Control, Communications and Intelligence) (OASD(C3I)).

The guidance for budget formulation and congressional justification for information technology programs, currently found in the DoD Financial Management Regulation (DoD 7000.14-R), Volume 2B, Chapter 18, will be reissued and maintained by OASD(C3I).

An Under Secretary of Defense (Comptroller) memorandum dated September 2, 1997 provided that OMB Circular A-11, Exhibit 43 series budget exhibits be delivered to OASD(C3I), Room 3D228, The Pentagon. DoD Components should continue to follow the guidance established in DoD 7000.14-R for preparation of Exhibit 43 series budget exhibits and deliver such budget exhibits to Room 3D228, The Pentagon unless advised otherwise by the OASD(C3I).


Belkis Leong-Hong
Deputy Assistant Secretary of Defense
for Plans and Resources, (C3I)


Nelson Toye
Deputy Chief Financial Officer
Office of the Under Secretary of Defense
(Comptroller)



2927

Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Financial Officer Comments



OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION
INTEGRATION

April 29, 2005

MEMORANDUM FOR INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Reporting on DoD Capital Investment for Information Technology in
Support of the FY 2006 Budget Submission (Project N. D-2005AL-
0036)

Thank you for the opportunity to review the subject draft report. We have
attached our position regarding the recommendations contained within the report.
My point of contact is Bonnie Hammersley, (703) 695-3937,
Bonnie.Hammersley@osd.mil.

A handwritten signature in cursive script that reads "Cheryl J. Roby".

Cheryl J. Roby
Deputy Assistant Secretary of Defense
(Resources)

Attachment

Copy to:
OUSD(C)/Program/Budget



Response to Office of Inspector General Draft Audit Report, “Reporting on DoD Capital Investment for Information Technology in Support of the FY 2006 Budget Submission (Project N. D-2005AL-0036)”

Recommendation that the Under Secretary of Defense (Controller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks Information Integration (NII) improve the quality of information technology reporting of the Office of Management and Budget and Congress by:

IG Recommendation 1. a Advising the Office of Management and Budget that Component information technology budget request will not be submitted until:

a. DoD Components complete and correct inadequate Capital Investment Reports

Response: Nonconcur. The DoD and OMB conduct a concurrent review of the DoD’s budget at every juncture. As a result, unlike other federal agencies, DoD does not send the budget estimate to OMB. While the IT is a subset of the DoD budget, we do submit the associated budget exhibits as directed in the OMB Circular A-11.

We have taken actions to reduce/mitigate the number of incomplete or inaccurate Capital Investment Reports. These actions include building in more time to review and revise Exhibit 300s prior to the President’s Budget submission, evaluating tools to help facilitate report submissions, and working with OMB to better understand reporting requirements.

For those exhibit 300s that are on the OMB watchlist, there is constant dialogue with OMB and the program offices/services/agencies to correct deficiencies. The dialogue is critical to understanding what is “inadequate”.

The concurrent program and budget review and constant dialogue with OMB, render it neither feasible nor logical to withhold submission.

Revised

b. Required signed statement of compliance from Component Chief Information Officers and Chief Financial Officers accompany the requests.

Response: Nonconcur. There are firm dates for the President's Budget submission to OMB and Congress, so holding up the submission is not a viable option. However, as you correctly noted in the report, DoD Financial Management Regulation (FMR), Volume 2, Chapter 18, requires a statement of compliance be provided within 10 calendar days of the due date of the electronic submission of the program/budget submission in September, and within 10 calendar days after the FYDP has locked for the final submission for the President's Budget submission. NII will enlist the help of OUSD(C) to enforce the FMR.

IG Recommendation 2. Expanding the self-assessment process to include more time for DOD components to revise deficient investments before making the initial submission to the Office of Management and Budget.

Response: Concur: As mentioned in our response to Recommendation 1.a., NII built in time for the opportunity to revise the EX300s in the FY 06 President's Budget, and we intend to provide time for revisions for the FY 07 BES.

Additional Comments: The following corrections are provided to the DRAFT report.

Appendix B: The list of DoD Components submitting Statements of Compliance for the Budget Estimate Submission has several errors. DLA, TRICARE, AFIS and DCMA did in fact provide statements. It should also be noted that the list does not reflect the entire group of organizations required to provide statements. The electronic files have been forwarded via email to your office. The list should be corrected as follows for the final report

Blue - ASD(NII) accounting		Received
Navy		No
TRICARE Management Agency	Yes	TMA.pdf
Defense Logistics Agency	Yes	DLA.pdf
Defense Commissary Agency	No	
American Forces Information Service	Yes	AFIS.pdf

Defense Contract Management Agency	Yes	DCMA.pdf
Defense Information Systems Agency	No	
Army	Yes	ARMY.pdf
Air Force	Yes	AF.pdf
Defense Human Resource Activity	Yes	DHRA.pdf
Missile Defense Agency	Yes	MDA.pdf
Defense Finance Accounting Service	Yes	DFAS.PDF
US Transportation Command	Yes	TRANSCOM.pdf
Office of Secretary Of Defense	Yes	
Washington Headquarters Service	Yes	WHS.pdf
Defense Security Service	Yes	DSS.pdf
Defense Threat Reduction Agency	Yes	DTRA.pdf
National Defense University	Yes	NDU.doc
DoD Education Activity	Yes	DoDEA.pdf
Defense Advanced Research Projects Agency	No	
Defense Commissary Agency	No	
Defense Contract Audit Agency	No	
Defense Technical Information Center	No	**
Joint Staff	No	
National Geospatial Intelligence Agency	No	
National Security Agency	No	
US Special Operations Command	No	
Inspector General	No	

** Exhibit 300 submitted by DISA for 06BES.

Team Members

The Department of Defense Office of the Deputy Inspector General for Auditing, Acquisition and Technology Management prepared this report. Personnel of the Department of Defense Office of Inspector General who contributed to the report are listed below.

Kathryn M. Truex
Robert L. Shaffer
George A. Leighton
Robert R. Johnson
Tina N. Brunetti
Rebecca S. Courtade
Courtney E. Woodruff
James J. Buscaigio
Cindy L. Gavura