December 30, 2005

Information Technology Management

Security Status for Systems Reported in DoD Information Technology Databases (D-2006-042)

Department of Defense
Office of Inspector General

Quality *Integrity* *Accountability*

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

Acronyms

ASD(NII)/CIO	Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
CFO	Chief Financial Officer
CIO	Chief Information Officer
CIR	Capital Investment Report
DITPR	DoD IT Portfolio Repository
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GAO	General Accountability Office
IT	Information Technology
ITMA	Information Technology Management Application
OMB	Office of Management and Budget
OSD	Office of the Secretary of Defense
SNaP-IT	Select Native Programming - Information Technology
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer

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

December 30, 2005

MEMORANDUM FOR ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION/CHIEF INFORMATION OFFICER

SUBJECT: Report on Security Status for Systems Reported in DoD Information Technology Databases (Report No. D-2006-042)

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. The comments of the Deputy Assistant Secretary of Defense for Networks and Information Integration/Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, were partially or nonresponsive to most of the recommendations. Therefore, we request that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer provide additional comments on those recommendations by January 27, 2006.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudATM@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 Ms. Karen J. Lamar at (703) 604-9005 (DSN 664-9005). The team members are listed inside the back cover. See Appendix F for the report distribution.

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-2006-042 **December 30, 2005**
(D2005-D000AL-0156.000)

Security Status for Systems Reported in DoD Information Technology Databases

Executive Summary

Who Should Read This Report and Why? DoD managers to include, but not limited to, all Component Chief Information and Chief Financial Officers responsible for reporting and certifying security information in the Information Technology (IT) Registry and in the Information Technology Management Application (ITMA) and their follow-on databases, the DoD IT Portfolio Repository and Select Native Programming - IT, and program office and headquarters personnel responsible for inputting information into DoD IT databases should read this report to improve the quality of data being relied upon to make management and budget decisions.

Background. Improving IT security is one of the Office of Management and Budget's highest priorities in IT management. DoD reports the security status of mission critical, mission essential, and select mission support systems in the IT Registry database and budget data on their IT investments in the ITMA database. The IT Registry and ITMA are the only DoD-wide mechanisms in place that DoD managers have to report the security status of DoD Component IT systems. The DoD CIO Memorandum, "DoD Information Technology Registry Guidance for Fiscal Year 2005," December 21, 2004, required that all DoD Component Chief Information Officers update and maintain their respective Component's input to the IT Registry; certify that all mission critical and mission essential systems are included in the IT Registry to include at least 50 percent of all mission support systems by December 1, 2005 and 100 percent by September 30, 2006; and ensure consistency between the IT Registry and ITMA.

The IT Registry is intended to provide a DoD-wide inventory of mission critical, mission essential, and select mission support systems and contains data elements which are populated by DoD Components that provide the security status of their IT systems. The IT Registry is used to report to the Office of Management and Budget and to Congress on the effectiveness of DoD Component and DoD-wide security programs. All systems included in the IT Registry will be merged into the DoD IT Portfolio Repository by January 31, 2006, in accordance with guidance issued by the Deputy Chief Information Officer on September 28, 2005.

ITMA was the authoritative source for DoD IT budget information through completion of the Department's FY 2006 IT budget preparation and submission. The follow-on database, Select Native Programming – IT, will be used as the authoritative source for FY 2007 and beyond. DoD Components must submit an Exhibit 300, "Capital Investment Report," for all major IT investments. DoD uses ITMA to plan, coordinate, and disseminate DoD IT budget exhibits and as the primary means of justifying and managing IT investments. DoD Components use the CIR to show management and the Office of Management and Budget 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.

Results. DoD Components did not accurately report the same IT system security data in the IT Registry and the ITMA databases. Specifically, 120 of 148 IT systems (81 percent) reported in FY 2006 President's Budget Capital Investment Reports did not match to reports on the same

systems in the IT Registry and 87 of 148 IT Registry reports (59 percent) were not internally consistent between the system mission criticality and the mission assurance category data elements. Additionally, DoD Components did not submit timely, accurate, or complete IT Registry certification and ITMA compliance statements to the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer. As a result, DoD, the Office of Management Budget, and Congressional Committees are making management decisions concerning technology operations, investments, security, interoperability, and architecture, based upon erroneous information contained in DoD databases.

Recommendations made in two prior DoD Office of the Inspector General audit reports identified weaknesses in management controls for accurate, consistent, and efficient reporting of IT system information in DoD IT databases. Those recommendations, if implemented, would have addressed part of the cause discussed in the Finding section of this report.

We recommend that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer ensure that information in DoD IT databases is accurate and complete. Specifically, we recommend that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer immediately commence utilization of automatic data integrity controls on DoD-wide IT databases; identify and impose penalties on those DoD Component Chief Information Officers that did not implement controls, reconcile DoD databases at least quarterly, and populate all required data elements; impose sanctions beginning first quarter FY 2006 on those DoD Components that do not submit an IT Registry/DoD Information Technology Portfolio Repository certification statement prior to the due date stating that their Component information is complete and correct; require DoD Component Chief Information Officers to submit IT Registry/DoD Information Technology Portfolio Repository certifications prior to submitting the DoD Federal Information Security Management Act Report to the Office of Management and Budget; advise the Office of Management and Budget and Congress that DoD does not have viable internal controls over the accuracy of data it is reporting concerning the security of its IT systems; develop internal control mechanisms, report the DoD database discrepancies as a material control weakness, and develop a plan to track and correct conditions; and adopt National Institute of Standards and Technology Standards to categorize their IT systems. See the Finding section of the report for detailed recommendations.

Management Comments and Audit Response. The comments of the Deputy Assistant Secretary of Defense for Networks and Information Integration/Deputy Chief Information Officer, responding for the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer, were partially responsive or nonresponsive to most of the recommendations. See the Finding section of the report for a discussion of management comments on the recommendations 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 Information Integration/Chief Information Officer comment on this report by January 27, 2006.

Table of Contents

Executive Summary i

Background 1

Objectives 2

Finding

DoD Information Technology Databases 4

Appendixes

A. Scope and Methodology 21
B. Prior Coverage 22
C. Information Technology Registry Systems Reviewed 24
D. Mission Assurance Category and Mission Criticality Definitions 30
E. Summary of Data Elements and DoD Components Reviewed 31
F. Report Distribution 32

Management Comments

Assistant Secretary of Defense for Networks and Information Integration/ Chief Financial Officer 35

Background

Improving information technology (IT) security is one of the Office of Management and Budget's (OMB) highest priorities in IT management. In addition, Congress has challenged the quality of DoD IT management because IT documents and associated budget data that DoD provided were inaccurate, misleading, or incomplete. DoD reports the security status of their mission critical, mission essential, and select mission support systems in the IT Registry database and budget data on their IT investments in the Information Technology Management Application (ITMA) database. The IT Registry and ITMA are the only DoD mechanisms in place that managers DoD wide have to report the security status of DoD Component IT systems. Both databases are in a state of flux and are scheduled to be replaced by the DOD IT Portfolio Repository (DITPR) and the Select Native Programming – Information Technology (SNaP-IT) respectively in FY 2006. The Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer (ASD[NII]/CIO), is the principal staff assistant to the Secretary of Defense for DoD IT.

The DoD CIO Memorandum, "DoD Information Technology Registry Guidance for Fiscal Year 2005," December 21, 2004, required that all DoD Component Chief Information Officers (CIOs) update and maintain their respective Component's input to the IT Registry on at least a quarterly basis; certify that all mission critical and mission essential systems are included in the IT Registry and enter at least 50 percent of all mission support systems by December 1, 2005, 75 percent by March 1, 2006, and 100 percent by September 30, 2006; and ensure consistency between DoD wide databases, such as the IT Registry, DITPR, ITMA, and SNaP-IT.

Information Technology Registry. The IT Registry is used as the official DoD database to meet external and internal reporting requirements. The IT Registry is intended to provide a DoD-wide inventory of mission critical and mission essential systems, and by September 30, 2006, will include all mission support systems. The IT Registry contains fields or "data elements" which are populated by DoD Components that provide a security status on their IT systems for such items as accreditation requirements; risk management, security, and incident response plans; and security control test information.

Information in the IT Registry is being used in FY 2005 to compile reports required by the Federal Information Security Management Act (FISMA) of 2002. Specifically, data elements in the IT Registry are used to compile the annual report to OMB and Congress on the effectiveness of DoD security programs, the quarterly report to OMB on the agency system and program metrics, and the E-Authentication Report and Privacy Act Assessments, which implement the E-Government Act.[1] During FY 2005, DoD planned to merge the IT Registry with the DITPR database, which will become the official unclassified DoD data source for FISMA; E-Authentication; Portfolio Management; Privacy Impact Assessments; the inventory

[1]The E-Government Act enhances the management and promotion of electronic Government services and processes by establishing a Federal CIO within OMB. It also establishes a broad framework of measures that require using Internet-based IT to enhance citizen access to Government information and services and to ensure privacy.

of mission critical, mission essential, and mission support systems; and the registry for systems under the DoD Instruction 5000.2.

Information Technology Management Application. DoD uses ITMA to plan, coordinate, and disseminate DoD IT Exhibit 300 Reports[2] (Capital Investment Reports [CIRs]) as required by OMB and Congress. For the FY 2006 President's Budget Request, ASD(NII)/CIO forwarded 172 CIRs, totaling $30 billion, to OMB. The CIR is the primary means of justifying and managing major IT investments. 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 IT investments. The Clinger-Cohen Act requires executive agencies to establish goals for improving the efficiency and effectiveness of agency operations through the effective use of IT and to submit an annual report to Congress on its progress in achieving those program goals. DoD uses the CIR to meet that annual reporting requirement to Congress.

DoD Regulation 7000.14-R, "Financial Management Regulation," volume 2b, chapter 18, "Information Technology Resources and National Security Systems," June 2004, required all DoD Components that have any resource obligations for IT or national security systems to submit a CIR that is complete, accurate, and consistent with the requirements of the Clinger-Cohen Act and OMB Circular A-11, "Preparation, Submission, and Execution of the Budget," part 7, section 300, "Planning, Budgeting, Acquisition, and Management of Capital Assets," July 2004. DoD Components must submit an Exhibit 300 or CIR for all major IT investments.[3] DoD Components use the CIR to show management and OMB 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 CIR should be complete and accurate and provide all required information to OMB.

In FY 2005, DoD began transitioning from ITMA to the SNaP-IT database, which is being utilized for the collection and reporting of FY 2007 IT budget information.

Objectives

The overall audit objective was to assess the consistency of information that DoD Components report to the Office of the Secretary of Defense (OSD), OMB, and Congress on the security status of their IT systems. Specifically, the audit determined whether information in ITMA, which is used to prepare the DoD IT budget request and CIRs, is consistent with system security information in the IT Registry, which is

[2] An Exhibit 300 is also referred to as a CIR.

[3] Major IT investments require special management attention because of their importance to an agency's mission, are for financial management and more than $500,000, have high executive visibility, and are defined as major investments by the agency's capital planning and investment control process.

used to prepare the DoD FISMA Report, and in accordance with OMB and DoD guidance. See Appendix A for discussion of the scope and methodology.

Management Controls

We did not review management's self-evaluation over the adequacy of their management controls. The audit focused on the accuracy of reporting security information by DoD Components in the IT Registry and ITMA databases. We identified that management at all levels omitted material internal controls that would ensure that security information in DoD databases was consistent. Specifically, data elements in the IT Registry and the ITMA databases did not identify the same information for the same system and therefore, did not demonstrate that the DoD CIO and Chief Financial Officer (CFO) communities had implemented sufficient controls to ensure that the reporting of system security information in those databases was accurate and complete. See the Finding section of the report for detailed discussions of the management control weaknesses.

DoD Information Technology Databases

DoD Components did not accurately report the same IT system security data in the IT Registry and ITMA databases. We reviewed the security data elements for 148 IT systems reported in both databases and determined that:

- 120 systems (81 percent) reported in the IT Registry did not match their corresponding CIRs in ITMA; and
- 87 IT Registry reports (59 percent) were not internally consistent between the system mission criticality and the mission assurance category data elements.

Additionally, DoD Components did not submit timely, accurate, or complete IT Registry certifications and ITMA compliance statements to the ASD(NII)/CIO. The IT system security data elements were not correctly reported because the Component CIO and CFO communities did not enact sufficient controls or conduct reviews to ensure that information in FY 2006 CIRs and in IT Registry Reports was the same information being reported in both databases. As a result, DoD, OMB, and Congressional Committees may be making management decisions concerning technology operations, investments, security, interoperability, and architecture, based upon erroneous information contained in the IT Registry and ITMA databases, which are used by DoD as the only means to report the security status of their IT systems and for making enterprise-wide investment and budgetary decisions.

DoD Information Technology Reporting

The DoD CIO Memorandum, "DoD Information Technology Registry Guidance for Fiscal Year 2005," December 21, 2004, required all DoD Component CIOs to ensure consistency between DoD databases, such as the IT Registry, DITPR, and ITMA. DoD Component security-related data element entries in ITMA and the IT Registry databases did not demonstrate that DoD CIOs were ensuring consistency and synchronization of Component system data in both databases. Specifically, 120 of 148 IT systems (81 percent) reported in IT Registry reports with corresponding FY 2006 CIRs showed that the same security data elements in both reports were either inconsistent or missing for testing, accreditation, and planning information. See Appendix C for listing of DoD IT systems reviewed.

Security Control Test Date. For all IT systems, DoD Components are required to provide the date of the most recent security control test performed for data elements in both the IT Registry and ITMA. However, for 112 of 148 IT systems (76 percent) reviewed, the security control test date data element was not consistent between the IT Registry and ITMA. Specifically, 77 of 112 IT Registry and ITMA reports identified a security control test date; however, the dates did not match. Additionally, 21 IT Registry reports did not identify a security control test date when the corresponding ITMA CIR did, 2 ITMA CIRs did not identify a security control test date when the corresponding IT Registry report contained a date, 8 IT Registry and ITMA reports contained no responses for the security control test date, and

3 IT Registry reports identified dates for when the system's last security control tests occurred; however, the ITMA CIR explicitly stated that the systems had not been tested for security. Lastly, one IT Registry report stated "not applicable" for the security control test date data element, while its corresponding ITMA CIR stated that the system had been tested. Table 1 identifies the discrepancy between IT Registry reports and ITMA CIRs for the security control test date data element.

Table 1. Comparison of the Security Control Test Date Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	27	84.4
Navy	33	27	81.8
Air Force	19	15	78.9
Defense Agencies	64	43	67.2
Total	**148**	**112**	**75.7***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Accreditation Date. DoD Components are required to identify the date an IT system has been accredited, or certified to operate, in IT Registry and ITMA Capital Investment Reports. Of 148 IT systems reviewed, 49 ITMA CIRs (33 percent) did not match corresponding IT Registry reports for the accreditation date data element. Specifically, 30 of 49 ITMA CIRs identified dates that did not match IT Registry reports, 5 IT Registry reports and 13 ITMA CIRs provided no response, and 1 IT Registry report stated that the accreditation date data element was "not applicable" when the corresponding ITMA CIR contained an accreditation date. Table 2 identifies the discrepancy between IT Registry and ITMA Capital Investment Reports for the accreditation date data element.

Table 2. Comparison of the Accreditation Date Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	12	37.5
Navy	33	12	36.4
Air Force	19	8	42.1
Defense Agencies	64	17	26.6
Total	**148**	**49**	**33.1***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Accreditation Status. DoD Components are required to provide the accreditation status for systems in all IT Registry and ITMA Capital Investment Reports that have undergone a certification and accreditation process. Systems that have undergone a certification and accreditation process may be granted an authority to operate, an interim authority to operate, an interim authority to test, or a denial of authority to operate. Of the 148 IT systems reviewed, 19 ITMA CIRs (13 percent) did not match corresponding IT Registry reports for the accreditation status data element. Specifically, 13 of those 19 systems did not report the same accreditation status in IT Registry and ITMA Capital Investment Reports, 1 ITMA CIR and 3 IT Registry reports left the accreditation status data element blank, and 2 IT Registry reports stated that the accreditation data element was "not applicable" when the corresponding ITMA CIRs stated that the systems had an interim authority to operate. Table 3 identifies the discrepancy between IT Registry and ITMA Capital Investment Reports for the accreditation status data element.

Table 3. Comparison of the Accreditation Status Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	5	15.6
Navy	33	6	18.2
Air Force	19	5	26.3
Defense Agencies	64	3	14.1
Total	**148**	**19**	**12.8***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Accreditation Method. DoD Components are required to report the standard used when accrediting an IT system. DoD Directive 8500.1, "Information Assurance," October 24, 2002, requires that all DoD IT systems utilize the DoD Information Technology Security Certification and Accreditation Process (DITSCAP) to grant certification and accreditation to any DoD IT system. The accreditation methodology data element for 12 of 148 ITMA CIRs (8 percent) reviewed did not match information in corresponding IT Registry reports. Specifically, six IT Registry reports and two ITMA CIRs did not provide a response for the accreditation method data element, one IT Registry report and its matching ITMA CIR identified differing accreditation methods, and three IT Registry reports stated "not applicable" when their corresponding ITMA CIRs identified that the DITSCAP was used. Table 4 identifies the discrepancy between the IT Registry reports and ITMA CIRs for the accreditation method data element.

Table 4. Comparison of the Accreditation Method Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	2	6.3
Navy	33	2	6.1
Air Force	19	4	21.1
Defense Agencies	64	4	6.3
Total	**148**	**12**	**8.1***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Accreditation Required. DoD Components are required to state in IT Registry and ITMA Capital Investment Reports whether a system is required to complete a DoD-approved IT security certification and accreditation process. The data element for whether an accreditation was required for 6 of the 148 ITMA CIRs (4 percent) reviewed was not consistent with corresponding IT Registry reports. Specifically, four of the six IT Registry reports stated that an accreditation was not required when the corresponding ITMA CIRs stated that it was, one IT Registry report did not provide a response for the accreditation required data element when the ITMA CIR stated that the accreditation was required, and the last IT Registry report stated that accreditation was required when the corresponding CIR stated that it was not. Table 5 identifies the discrepancy between IT Registry reports and ITMA CIRs for the accreditation required data element.

Table 5. Comparison of the Accreditation Required Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	1	3.2
Navy	33	2	6.1
Air Force	19	2	10.5
Defense Agencies	64	1	1.6
Total	**148**	**6**	**4.1***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

System Security Authorization Agreement Status. For each IT system, the IT Registry and ITMA Capital Investment Reports provided a system security authorization agreement status, which is based on the method used to certify and accredit that an IT system has the authority to operate. The DITSCAP is used to certify and accredit a DoD IT system and is divided into four phases. Sixteen of the 148 ITMA CIRs (11 percent) reviewed did not match to the phase being reported in corresponding IT Registry reports. Specifically, information for the system security authorization agreement status for 3 of 16 ITMA CIRs did not agree with the corresponding IT Registry report, 12 IT Registry reports did not provide a response for system security authorization agreement status data element, and 1 IT Registry report stated "not applicable" for the system security authorization agreement status data element. Table 6 identifies the discrepancy between IT Registry reports and ITMA Capital Investment Reports for the system security authorization agreement status data element.

Table 6. Comparison of the System Security Authorization Agreement Status Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	4	12.5
Navy	33	8	24.2
Air Force	19	2	10.5
Defense Agencies	64	2	3.1
Total	**148**	**16**	**10.8***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Risk Management Plan. DoD Components are required to report whether an IT system has a risk management plan. That plan identifies the risks and vulnerabilities associated with the system, assesses the sensitivity of the data, and identifies the approach to mitigate those risks and vulnerabilities. For 16 of the 148 ITMA CIRs (11 percent) reviewed, the corresponding IT Registry reports for the risk management plan data element did not match. Specifically, 10 IT Registry reports did not provide a response for the risk management plan data element when the ITMA CIR identified that there was a plan for the system, and 4 IT Registry reports stated that the plan was "not applicable" when the corresponding ITMA CIRs stated that a risk management plan was in place. Additionally, two IT Registry reports stated that there was no risk management plan for the system, while the corresponding ITMA CIR explicitly stated that there was a plan. Table 7 identifies the discrepancy between IT Registry and ITMA Capital Investment Reports for the risk management plan data element.

Table 7. Comparison of the Risk Management Plan Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	5	15.6
Navy	33	3	9.1
Air Force	19	2	10.5
Defense Agencies	64	6	9.4
Total	**148**	**16**	**10.8***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Security Plan. DoD Components are required to state whether each IT system has a system security plan. The system security plan provides an overview of the security requirements of the system and describes the controls in place or planned for meeting those requirements. Sixteen of the 148 ITMA CIRs (11 percent) reviewed did not match the corresponding IT Registry reports for the security plan data element. Eleven of the 16 ITMA CIRs had blank security plan information in their IT Registry reports, and three ITMA CIRs provided a response that did not match IT Registry reports. Two IT Registry reports stated that a security plan was "not applicable" when corresponding ITMA CIRS identified that a security plan was in place. Table 8 identifies the discrepancy between IT Registry reports and ITMA CIRs for the security plan data element.

Table 8. Comparison of the Security Plan Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	5	15.6
Navy	33	5	5.2
Air Force	19	2	10.5
Defense Agencies	64	4	6.3
Total	**148**	**16**	**10.8***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Security Incident Response Plan. DoD Components are required to report whether their IT systems had controls in place to recognize, report, monitor, and efficiently handle security incidents and share this information with the appropriate organizations. Fifteen of the 148 ITMA CIRs (10 percent) reviewed did not match corresponding IT Registry reports for the security incident response plan data element. Specifically, 11 of 15 IT Registry reports did not record a response for the security incident response plan data element, 2 IT Registry reports and their corresponding ITMA CIRs provided responses that did not match, and 2 IT Registry reports stated that a security incident response plan was "not applicable" when the corresponding ITMA CIRs identified that a security incident response plan was in place. Table 9 identifies the discrepancy between IT Registry and ITMA Capital Investment Reports for the security incident response plan data element.

Table 9. Comparison of the Security Incident Response Plan Data Element Between IT Registry and ITMA Capital Investment Reports

	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	5	15.6
Navy	33	3	9.1
Air Force	19	2	10.5
Defense Agencies	64	5	7.8
Total	**148**	**15**	**10.1***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Mission Assurance Category and Mission Criticality. DoD Directive 8500.1, "Information Assurance," October 24, 2002, defines the mission assurance categories

and the Deputy CIO Memorandum, "Department of Defense Information Technology Registry Guidance for Fiscal Year 2005," December 21, 2004, defines mission critical, mission essential, and mission support systems (based on requirements found in DoD Instruction 5000.2, "Operation of Defense Acquisition System," May 12, 2003). See Appendix D for definitions of mission assurance categories and mission criticalities from the source documents. The relationship between the definitions is the importance of potential impact should the system become inoperable. For example, if a mission assurance category I or mission critical system would lose capability that loss would severely impact operations. If a mission assurance category II or mission essential system lost system capability, an organization or mission could sustain operations a short period before seriously impacting those operations, and the loss of capability for a mission assurance category III or mission support system would not significantly impact mission effectiveness or operational readiness. The relationship between mission assurance and mission criticality for 87 of 148 IT Registry Reports (59 percent) was not consistent. Of the 87 IT Registry Reports:

- 37 reports designated the IT system as mission essential with a mission assurance category III;
- 18 reports designated the IT system as mission critical with a mission assurance category II;
- 13 reports did not designate a mission assurance category;
- 11 reports designated the IT system as mission critical with a mission assurance category III;
- 4 reports designated IT system as mission essential with a mission assurance category I;
- 2 reports indicated that the mission assurance category was "not applicable;"
- 1 report designated the IT system as mission support with a mission assurance category I; and
- 1 report designated the IT system as mission support with a mission assurance category II.

Table 10 identifies the discrepancy between the mission assurance category and mission criticality data elements in the IT Registry.

Table 10. Comparison Between Mission Assurance Category and Mission Criticality Data Element in IT Registry Reports			
	Systems Reviewed	System Reports Did Not Agree	Percent
Army	32	12	37.5
Navy	33	23	69.7
Air Force	19	12	63.2
Defense Agencies	64	40	62.5
Total	**148**	**87**	**58.8***

*This is the percent of the total system reports that did not agree and the total systems reviewed.

Appendix C identifies the 148 IT systems reviewed and those systems with inaccurate and incomplete information for security data elements in the IT Registry and in ITMA and the inconsistencies between the mission assurance and mission criticality categories in IT Registry reports.

The inconsistencies identified would not have occurred if the DoD were compliant with Federal Information Processing Standards Publication (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems," February 2004. OMB FISMA reporting guidance for both FY 2004 and FY 2005 required all Federal agencies to report the security categorization of their IT systems in accordance with the FIPS 199 three levels of potential impact on organizations or individuals should there be a breach of security (i.e., a loss of confidentiality, integrity, or availability). These impact levels are: low, moderate, and high. All agencies must categorize their information and information systems using one of those three categories in order to determine which security controls should be implemented. Because DoD is not compliant with FIPS 199, on April 18, 2005, the Acting ASD(NII)/CIO directed that the mission assurance category level categorizations found in DoD Instruction 8500.2 be utilized to report the status of DoD IT systems populating the IT Registry for FY 2005 FISMA reporting purposes. However, the IT Registry is populated by systems in accordance with their mission critical, mission essential, or mission support status, and the data elements are not necessarily consistent. Adoption of the OMB and Congressionally directed FIPS 199 will both resolve this internal DoD inconsistency and preclude aggregation of inconsistent data across the Federal agency spectrum.

DoD IT Database Certification and Compliance Statements

DoD Components did not adhere to DoD policy and guidance when preparing compliance and certification statements. Specifically, DoD Components did not submit timely, accurate, or complete IT Registry certifications and ITMA compliance statements to ASD(NII)/CIO.

Information Technology Registry Certification Statement. The Deputy CIO Memorandum, "DoD Information Technology Registry Policy Guidance for 2004," December 1, 2003, required that the DoD Component CIO certify in writing that all IT systems—including mission critical and mission essential financial IT systems—were properly registered in the IT Registry and that all required data elements were correct; however, the FY 2005 Deputy CIO Memorandum did not. The FY 2005 Deputy CIO Memorandum included a certification template which recommended that the Component CIO state that changes to mission critical and mission essential systems were complete and correct; however, the FY 2005 policy memorandum did not require that the Component CIO explicitly state in their certification letter that the data elements for all systems, regardless of change, were complete and correct as did the FY 2004 guidance.

We reviewed 41 DoD Components for FY 2004 IT Registry certification statements and identified that 10 Components (24 percent) did not submit a certification for their IT systems. Twenty-eight of 31 Components that submitted certification statements stated that all their IT systems were registered in the IT Registry; however, only 8 Components certified that all required data elements were correct. Additionally, 24 of the 31 Components (77 percent) submitted certification statements were dated after the July 15, 2004, due date and 4 certifications were not dated.

For FY 2005, the ASD(NII)/CIO required in the Deputy CIO Memorandum, "DoD Information Technology Registry Guidance for Fiscal Year 2005," December 21, 2004, that DoD Component CIOs complete their last update to the IT Registry no later than September 1, 2005, six weeks after the July 22, 2005 due date for the submission of the DoD Component FISMA reports to OSD. Additionally, ASD(NII)/CIO required that DoD Components provide written IT Registry certifications covering the period October 1, 2004, through September 30, 2005, by October 15, 2005, one week after the October 7, 2005, deadline for submission of the Department-wide FISMA report to OMB. ASD(NII)/CIO did not enact sufficient controls to ensure the accuracy of information in the IT Registry—used to support the DoD FISMA reports to OMB and Congress—because IT Registry updates and required certification statements were permitted after submission of the consolidated DoD report to OMB. The DoD report to OMB is based on system data uncertified by DoD Components, and OSD has no other internal control mechanism for validating the data utilized for management purposes by OSD, OMB, and Congress.

Capital Investment Report Statements of Compliance. DoD Regulation 7000.14-R, volume 2b, chapter 18, required that the DoD Component CIO and CFO sign a joint memorandum stating that their budget submissions were complete; accurately aligned with the primary budget, program and/or acquisition materials; and consistent with the Clinger-Cohen Act, OMB Circular A-11, the DoD CIO guidance memorandums, and the Paperwork Reduction Act. The FY 2006 Budget Estimate Submission statements of compliance were due to ASD(NII)/CIO on September 9, 2004.

All DoD DoD Components were required to submit statements of compliance for their IT budget requests, but not all Components had major investments requiring preparation of an ITMA CIR. Of the 15 Components that submitted ITMA CIRs, 13 Components submitted statement of compliance memorandums for their investment information in ITMA, while the Navy and the Defense Commissary

Agency did not. However, only 2 of the 13 statements were dated on or before the September 9, 2004 due date; 4 of the 13 statements were not signed by both the CIO and the CFO; and 7 statements did not include the required statements that their budget submissions were complete; accurately aligned with the primary budget, program and or acquisition materials; and consistent with DoD and OMB guidance.

Management Controls Over DoD IT Databases

Information technology system security data elements were not correctly reported in DoD databases because the CIO and CFO communities did not enact sufficient controls or conduct reviews to ensure that the same information was being reported in the IT Registry and ITMA. Recommendations made in two prior DoD IG audit reports identified weaknesses in management controls for accurate, consistent, and efficient reporting of IT system information in DoD IT databases and recommended that the Under Secretary of Defense (Comptroller)/Chief Financial Officer (USD[C]/CFO) and the ASD(NII)CIO enact such controls to mitigate those management weaknesses. Those recommendations, if implemented, would have assisted USD(C)/CFO and ASD(NII)/CIO to implement controls that would have addressed part of the cause discussed in the Finding section of this report.

DoD IG Report No. D-2003-117, "Systems Inventory to Support the Business Enterprise Architecture," July 10, 2003, recommended the Office of USD(C)/CFO and ASD(NII)/CIO, as part of the Business Modernization and Systems Integration Governance Concept, establish procedures to verify through the architecture domain owners that the data included in the architecture domain database mirror what is included in the IT Registry and any other databases maintained for systems in a particular domain and that the completeness of the data be verified periodically to ensure that the data was kept current, consistent, and accurate to enhance budget decisions and respond to OMB and Congressional reporting requirements. USD(C)/CFO and ASD(NII)/CIO responded on August 15, 2003, that the Department would create an "integrated repository" that would allow the use of current data structures already developed for the IT Registry, the Business Management Modernization Program database, and ITMA to use a single source update to post information to all databases, thus ensuring equality of data for updating the databases. The intent of the "integrated repository" was to use a single source update process to post information to all databases. USD(C)/CFO and ASD(NII)CIO also stated that the common data currently maintained in the IT Registry, the Business Management Modernization Program database, and ITMA would be reconciled to ensure that the initial baseline of data included in the integrated data repository agrees.

As of October 2005, the "integrated repository" had not been developed, although work is underway to form an IT Management Data Community of Interest at some future time. With passage of the National Defense Authorization Act for FY 2005, section 332, responsibility for management oversight of the Defense business information systems has transferred from USD(C)/CFO to the Defense Business System Management Committee chaired by the Deputy Secretary of Defense. Responsibility to ensure that consistent and accurate information is being reported in

DoD IT databases; however, remains with ASD(NII)/CIO as the proponent of both the IT Registry and ITMA (and follow-on databases DITPR and SNaP-IT).

DoD IG Report No. D-2003-008, "Implementation of the Government Information Security Reform by the Defense Finance and Accounting Service for the Defense Integrated Financial Systems," October 7, 2002, recommended that ASD(NII)/CIO (formally known as the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence) develop effective data integrity controls, in coordination with the DoD Components, that ensure the accuracy, completeness, and validity of information entered in the DoD IT Registry database (Recommendation 1.a.). DoD IG Report No. D-2003-008 also recommended that ASD(NII)/CIO reconcile, on an annual basis, the systems in the IT Registry with those reported by the DoD Component CIO (Recommendation 1.b.). ASD(NII)/CIO concurred with Recommendation 1.a. stating that they expect users to enter data correctly and that they rely on the user's internal business process to ensure accuracy, completeness, and validity of information. ASD(NII)/CIO also said that they would issue clarifying IT Registry guidance that would address Recommendation 1.a. ASD(NII)/CIO partially concurred with Recommendation 1.b. stating that DoD Component CIOs certify the accuracy of systems on an annual basis and that the new IT Registry guidance would require those Component CIOs to reconcile their mission critical and mission essential data on a quarterly basis and to certify the accuracy of information entered by their organizations.

ASD(NII)/CIO corrective actions to recommendations in DoD IG Report Nos. D-2003-117 and D-2003-008 remain insufficient to ensure that accurate and complete information is being reported in DoD databases used to report on the security status of DoD IT systems to OMB and to the Congress.

Conclusion

The IT system information maintained in the IT Registry and ITMA is unreliable because the DoD CIO and CFO communities failed to enact sufficient controls to ensure the accuracy, consistency and synchronization of Component system data between those DoD databases, as mandated in DoD guidance. In addition, DoD is not in compliance with NIST FIPS 199, "Standards for Security Categorization of Federal Information and Information Systems." The flawed information in the IT Registry and in ITMA is the only means for DoD to report the security status of their IT systems enterprise-wide and is being used to compile reports for FISMA, the Privacy Act, and the E-Authentication reporting requirements, as well as the DoD IT budget request and justification and the DoD response to the requirement of National Defense Authorization Act for FY 2005 section 332. DoD, OMB, and Congressional Committees are making enterprise-wide management decisions concerning IT operations, investments, security, interoperability, and architecture, based upon database reports containing erroneous information. The incorrect, inaccurate, and incomplete information in the current DoD IT databases diminishes the utility of those databases for management oversight purposes. Unless DoD management develops and enforces effective internal quality assurance controls over Component controlled data in the new DITPR and SNaP-IT databases, this situation will continue.

Recommendations, Management Comments, and Audit Response

We recommend that the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer ensure that the information in DoD information technology databases is accurate and complete. Specifically,

1. Immediately commence utilization of automatic data integrity controls on DoD-wide information technology databases to preclude population of data elements with invalid entries as recommended by the Office of the Inspector General in August 2002.

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred stating the DoD CIO plans to establish the DoD IT Management Data Community of Interest in December 2005 that will include a net-centric capability for publishing and subscribing to all authoritative IT management data. The process established by the Community of Interest will ensure that data elements across the department are populated and traceable.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments are partially responsive. We request the Deputy CIO provide detailed information on the Community of Interest initiative to include implementation schedule and responsible offices.

2. Identify and impose penalties beginning in the first quarter of FY 2006 on those DoD Component Chief Information Officers that did not:

Management Comments. The Deputy ASD(NII)/Deputy CIO nonconcurred with imposing penalties on the CIO stating that existing mechanism can be strengthened to enforce data integrity.

Audit Response. The Deputy ASD(NII)/Deputy CIO were nonresponsive. We request the Deputy ASD(NII)/Deputy CIO identify those current and new mechanisms that will be used to strengthen and enforce data integrity within and between DoD databases.

a. Implement sufficient controls to ensure that all common security data elements in the Information Technology Registry/DoD Information Technology Portfolio Repository and the Information Technology Management Application/Select and Native Programming Information Technology databases are the same;

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred stating that FISMA, DITPR, and IT budget guidance will reemphasize that each Component CIO is responsible for ensuring that all common security data elements in the IT Registry/DITPR and the ITMA/SNaP-IT databases are the same.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were nonresponsive. The issuance of guidance is the first step to implementing sufficient controls to ensure the commonality of security information in DoD databases;

however, additional controls are required as the inconsistencies in DoD databases has been an unresolved issue. We first highlighted the need for additional controls in DoD IG Report Nos. D-2003-008 and D-2003-117; however, those recommendations were not implemented. Therefore, we request the Deputy ASD(NII)/Deputy CIO reconsider this recommendation and implement sufficient controls to ensure that all common security data elements in the IT Registry/DITPR and ITMA/SNaP-IT are the same.

b. Reconcile the security data elements in the Information Technology Registry/DoD Information Technology Portfolio Repository and the Information Technology Management Application/Select and Native Programming Information Technology databases at least quarterly to ensure that they are the same; and

Management Comments. The Deputy ASD(NII)/Deputy CIO partially concurred stating because the IT budget data, collected in SNaP-IT, is done so bi-annually and that quarterly reconciliations would be inefficient and provide no benefit. She stated that DoD will establish an automated annual security data elements reconciliation process that will be institutionalized through the databases' Configuration Control Boards with results of corrective actions being reported to the DoD CIO and CIO Executive Board.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were partially responsive. The Deputy ASD(NII)/Deputy CIO did not state when she will establish the reconciliation process as part of the databases' Configuration Control Boards, results and status of necessary corrective action reporting.

c. Populate all required data elements in the Information Technology Registry/DoD Information Technology Portfolio Repository and the Information Technology Management Application/Select Native Programming – Information Technology databases.

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred stating that the DoD CIO is in the process of developing annual DITPR guidance, expected to be issued in December 2005, that will identify mandatory data elements that must be populated within 90 days. If uncorrected after 90 days, the system will be deleted from DITPR and identified to the DoD CIO. The Deputy ASD(NII)/Deputy CIO stated that ASD(NII), Resources Directorate, is in the process of identifying those data elements that are required in SNaP-IT and issuing those requirements to the SNaP-IT development team.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were responsive to the recommendation; therefore, no further comments are required.

3. Include the requirement in all future DoD Information Technology Portfolio Repository guidance that DoD Components explicitly certify in writing that the information in the DoD Information Technology Portfolio Repository is complete and correct.

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred stating that in response to the FY 2005 National Defense Authorization Act, the Department

recently issued a Concept of Operations for Investment Review Boards. That document provides the necessary detail regarding governance, roles, responsibilities, processes, controls, and reporting requirements to ensure that component IT investments are visible to the highest levels of DoD and are in compliance with mission area guidance and recommendations.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were nonresponsive. We request that the Deputy ASD(NII)/Deputy CIO provide additional comments on this recommendation as she did not state whether she would require, in all future DITPR guidance, that DoD Components explicitly certify in writing that the information in DITPR is complete and correct. Further, DITPR is the authoritative DoD database for all IT management data, to include the warfighting, intelligence, and enterprise information environment mission areas in addition to the defense business systems addressed by the FY 2005 National Defense Authorization Act.

4. Review the Information Technology Registry/DoD Information Technology Portfolio Repository certifications to ensure that DoD Components are submitting required certification. Identify and impose sanctions beginning in the first quarter FY 2006 on those DoD Components that do not:

a. Submit a certification prior to the due date;

b. Include a date on the certification statement; and

c. Explicitly state that the information in the Information Technology Registry/DoD Information Technology Portfolio Repository is complete and correct.

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred stating that those DoD CIO's who do not submit a certification prior to the due date, include a date on the certification statement, and explicitly state that the information in the IT Registry/DITPR is complete and correct, will be identified to the DoD CIO and required to explain their inactions to the DoD CIO Executive Board.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were responsive to the recommendation; therefore, no further comments are required.

5. Require DoD Components Chief Information Officers in FY 2006 and beyond to submit the Information Technology Registry/DoD Information Technology Portfolio Repository certifications prior to submitting the DoD Federal Information Security Management Act Report to the Office of Management and Budget.

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred stating that certifications will be required annually on the first of September.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were responsive to the recommendation; therefore, no further comments are required.

6. Advise the Office of Management and Budget and Congress that DoD does not have viable internal controls over the accuracy of data it is reporting concerning the security of its information technology systems and investments and caveat all reports based on data drawn from unreliable databases, such as the Information Technology Registry/DoD Information Technology Portfolio Repository and the Information Technology Management Application/Select Native Programming – Information Technology until such time as demonstrably effective internal controls have been in place for at least one full year reporting cycle.

Management Comments. The Deputy ASD(NII)/Deputy CIO nonconcurred stating that the FY 2007 Exhibit 300 review process has greatly improved the data quality of the security data submissions in the Exhibit300s. She stated that resource managers were briefed on findings identified by the DoD, Office of the Inspector General on the FY 2006 Exhibit 300s and all Component FISMA IA officials were briefed to review both databases for consistency for the FY 2007 submissions.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were nonresponsive. Although the Deputy ASD(NII)/Deputy CIO stated that the Exhibit 300 data quality has greatly improved and that IA officials were briefed to review consistency between the databases, the fact remains that internal controls are not effective to ensure the accuracy of reporting the security of DoD IT systems and investments as inconsistencies still remain. We request that the Deputy ASD(NII)/Deputy CIO explain the specific internal controls implemented to substantiate their conclusion that the FY 2007 Exhibit 300 review process has improved the data quality and that briefing Component FISMA officials regarding database consistency constitutes an effective internal control.

7. Develop internal control mechanisms other than Component Chief Information Officer and Chief Financial Officer certifications, report the discrepancies between DoD databases as a material control weakness, and develop a Plan of Action and Milestones to track and correct conditions.

Management Comments. The Deputy ASD(NII)/Deputy CIO concurred with the development of internal control mechanisms other than Component CIO and CFO certifications stating that the ITMA application is being re-hosted as a components of SNaP-IT. Once re-hosted, the Deputy Assistance Secretary of Defense for Resources and the Director, Program Analysis and Evaluation will work toward integrating the IT budget with the overall DoD budget and adequate management controls should be available to ensure alignment with the IT budget and the overall DoD budget and the Statement of Compliance can be eliminated.

The Deputy ASD(NII)/Deputy CIO nonconcurred with reporting discrepancies between DoD databases as a material control weakness and developing a Plan of Action and Milestone stating that the inconsistencies do not represent a material weakness and that ASD(NII)/CIO has thoroughly examined database requirements and identified areas to strengthen the integration of or interface between databases.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were nonresponsive. We request that the Deputy ASD(NII)/Deputy CIO provide the management controls that will be used to ensure alignment with the IT budget and the

overall DoD budget. Additionally, we request that the Deputy ASD(NII)/Deputy CIO reconsider reporting the discrepancies between authoritative DoD databases for the IT budget and IT data management as a material control weakness and not developing a Plan of Action and Milestone.

8. Adopt National Institute of Standards and Technology Federal Information Processing Standards Publication 199 to categorize information and information systems and revise the Information Technology Registry/DoD Information Technology Portfolio Repository and the Information Technology Management Application/Select Native Programming – Information Technology data elements accordingly.

Management Comments. The Deputy ASD(NII)/Deputy CIO nonconcurred stating that there are fundamental differences between FIPS 199 potential impact definitions and DoD Mission Assurance Categories and confidentiality requirements that DoD uses to categorize information systems. She explained that the difference is that FIPS 199 focuses on potential impact to the organization and is not applicable to National Security Systems while the Mission Assurance Category focuses on impact to operational readiness and mission effectiveness.

The Deputy ASD(NII)/Deputy CIO further stated that DoD IA policy promulgated in DoD Instruction 8500.2 is more stringent that FIPS 199 for confidentiality because FIPS 199 definition for MODERATE and HIGH impact equate to classified information for DoD which requires more stringent IA controls that also enhances integrity and availability by restricting both physical and logical access. The Deputy ASD(NII)/Deputy CIO stated that for integrity, DoD IA policy is more stringent because it requires absolute integrity at the FIPS 199 MODERATE and HIGH impact levels and that the availability controls can be compared to the three impact levels in FIPS 199 and appear essentially equivalent.

Audit Response. The Deputy ASD(NII)/Deputy CIO comments were nonresponsive to the recommendation; however, no further comments are required at this time. The subject of applicability of NIST standards and guidelines to DoD National Security Systems and non-IT National Security Systems is being pursued between the Deputy ASD(NII)/Deputy CIO and the DoD, Office of the Inspector General in a separate forum.

Appendix A. Scope and Methodology

We reviewed 172 CIRs found in ITMA that DoD submitted to OMB and the Congress with the FY 2006 President's Budget request. We determined that 148 CIRs were IT systems also being reported in the IT Registry for system security reporting purposes under FISMA. The remaining 24 CIRs were identified by program officials as infrastructure, an investment or initiative, or a mission support system; and therefore, were not reported in the IT Registry. We reviewed and compared responses for the following nine security-related data elements in the IT Registry and ITMA: security control test date, accreditation date, accreditation status, accreditation method, accreditation required, system security authorization agreement status, risk management plan, security plan, and security incident response plan. We also reviewed and compared responses in IT Registry individual system reports for mission assurance category and mission criticality data elements. We assessed the consistency of information in reports prepared by DoD Components in the ITMA and IT Registry databases, as well as the internal consistency of security data elements in the IT Registry. The Component data contained in those databases is utilized by OSD to manage the information assurance program of the Department and to make congressionally required reports regarding that program to OMB and Congress.

We reviewed DoD Component CIO IT Registry certification statements to identify whether all systems were properly registered in the IT Registry and that all required data elements were complete and accurate. We also reviewed ITMA CIR statements of compliance for certification that budget submissions contained required information and were in compliance with DoD policy and guidance.

We evaluated the reporting process and the completeness of information in IT reports, based on report preparation guidance from the Clinger-Cohen Act, OMB Circular A-11, DoD Regulation 7000.14-R, the DoD CIO FY 2004 and FY 2005 IT Registry guidance memorandums, FISMA, and the Paperwork Reduction Act. We reviewed relevant documents addressing IT reporting guidance for DoD databases dated from July 2004 through September 2005. We met with analysts responsible for IT budget reports and the IT Registry within ASD(NII) to obtain access to IT system reports and to understand the FY 2005 reporting process of the DoD IT systems in various databases.

We performed this audit from May 2005 through November 2005 in accordance with generally accepted government auditing standards.

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 the Protecting the Federal Government's Information-Sharing Mechanisms and the Nation's Critical Infrastructures high risk area.

Appendix B. Prior Coverage

During the last 5 years, the Government Accountability Office (GAO) and the Department of Defense Inspector General have issued 17 reports discussing the reliability of DoD IT budget submission. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report No. GAO-05-552, "Weaknesses Persist at Federal Agencies Despite Progress Made in Implementing Related Statutory Requirements," July 15, 2005

GAO Report No. GAO-05-381, "DoD Business System Modernization: Billions Being Invested Without Adequate Oversight," April 29, 2005

GAO Report No. GAO-04-858, "Defense Acquisitions: The Global Information Grid and Challenges Facing Its Implementation," July 28, 2004

GAO Report No. GAO-04-823, "Federal Chief Information Officers: Responsibilities, Reporting Relationships, Tenure, and Challenges," July 21, 2004

GAO Report No. GAO-04-615, "DoD Business System Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability," May 27, 2004

GAO Report No. GAO-04-731R, "DoD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments," May 17, 2004

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

DoD IG

DoD Inspector General Report No. D-2005-099, "Status of Selected DoD Policy on Information Technology Governance," August 19, 2005

DoD Inspector General Report No. D-2005-094, "Proposed DoD Information Assurance Certification and Accreditation Process," July 21, 2005

DoD Inspector General Report No. D-2005-083, "Reporting of DoD Capital Investments for Information Technology in Support of the FY 2006 Budget Submission," June 10, 2005

DoD Inspector General Report No. D-2005-054, "DoD Information Technology Security Certification and Accreditation Process," April 28, 2005

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 Milestone 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

DoD Inspector General Report No. D-2003-117, "Systems Inventory to Support the Business Enterprise Architecture," July 10, 2003

DoD Inspector General Report No. D-2003-008, "Implementation of the Government Information Security Reform by the Defense Finance and Accounting Service for the Defense Integrated Financial System," October 7, 2002

Appendix C. IT Registry and ITMA Systems Reviewed

		Inconsistent Data Between:	
		IT Registry and ITMA CIRs	IT Registry Mission Assurance and Criticality Categories
	Army Systems		
1	Advanced Field Artillery Tactical Data System	no	no
2	All Source Analysis System	yes	no
3	Army Airborne Command and Control System	yes	no
4	Battle Command Sustainment Support System	yes	no
5	Combat Terrain Information System	yes	no
6	Defense Message Service – Army	yes	yes
7	Distributed Learning System	no	no
8	Distributive Training Technology	yes	no
9	Electronic Military Personnel System	yes	yes
10	Enhanced Position Location Reporting System	yes	no
11	Enterprise Human Resources System	yes	yes
12	Force XXI Battle Command Brigade and Below	yes	no
13	Forward Area Air Defense Command and Control System	yes	no
14	General Fund Enterprise Business System	yes	no
15	Global Combat Support System – Army	yes	no
16	Global Command and Control System – Army	no	no
17	Guardnet XXI, The Army National Guard's Wide Area Network	yes	no
18	Installation Support Module	yes	yes
19	Joint Computer-Aided Acquisition and Logistics Support	yes	yes
20	Joint Tactical Radio System – Cluster 1	yes	yes
21	Joint Tactical Radio System – Joint Program Office (JPO)	yes	yes
22	Logistics Modernization Program	yes	yes
23	Maneuver Control System	yes	no
24	Personnel Enterprise Support – Automation	yes	yes
25	Reserve Component Automation System	yes	yes
26	Secure Mobile Anti-Jam Reliable Tactical-Terminal	yes	no
27	Single Channel Ground and Airborne Radio System	yes	no
28	Tactical Operation Centers	yes	yes

		Inconsistent Data Between:	
		IT Registry and ITMA CIRs	IT Registry Mission Assurance and Criticality Categories
	Army Systems (cont'd)		
29	Transportation Coordinators' Automated Information for Movements System II	no	no
30	US Army Accessions Command Integrated Automation Architecture	yes	no
31	US MEPCOM Integrated Resource System	yes	yes
32	Warfighter Information Network - Tactical	yes	no
	Navy Systems		
1	Automated Teller Machines – At Sea	yes	no
2	Aviation Supply Chain and Maintenance – Enterprise Resource Planning	no	yes
3	Baseline Advanced Industrial Management Express	yes	yes
4	Claimant Financial Management System	yes	yes
5	Deployable Joint Command and Control	yes	no
6	Electronic Acquisition 21	yes	yes
7	Electronic Commerce/Electronic Data Interchange	yes	no
8	Electronic Military Personnel Records System	no	yes
9	Finance and Air Clearance Transportation System	yes	yes
10	Global Combat Support System – Marine Corps	yes	yes
11	Global Command and Control System – Maritime	yes	no
12	Maritime Corps Total Force System – Personnel	yes	yes
13	Material Finance Control System	no	no
14	Military Sealift Command Financial Management System	no	no
15	Multifunctional Information Distribution System – Low Volume Terminal	yes	yes
16	Navair Depot Maintenance System	yes	yes
17	Navair Program Management - Enterprise Resource Planning	yes	yes
18	Navsea Navy Enterprise Maintenance Automated Information System – Enterprise	no	yes
19	Navy Air Force Interface	yes	yes
20	Navy.com	yes	no
21	Navy Distance Learning System	yes	yes
22	Navy Enterprise Resource Planning	yes	no

		Inconsistent Data Between:	
		IT Registry and ITMA CIRs	IT Registry Mission Assurance and Criticality Categories
	Navy Systems (cont'd)		
23	Navy Marine Corps Intranet (NMCI)	yes	yes
24	Navy Mission Planning System	yes	yes
25	Navy Standard Integrated Personnel System	yes	yes
26	Navy Tactical Command Support System	yes	no
27	Shipyard Management Information Systems – Infrastructure	yes	yes
28	SPAWAR Financial Management – Enterprise Resource Planning	yes	yes
29	Standard Labor Data Collection and Distribution Accounting	yes	yes
30	Support Equipment Resource Management Information System	yes	no
31	Trident Logistics Data System	yes	yes
32	Uniform ADP – Inventory Control Points	yes	yes
33	Uniform ADP System – Stock Points	yes	yes
	Air Force Systems		
1	Advanced Distributive Learning System	yes	no
2	Air Force Mission Support System	yes	yes
3	Battle Control System – Mobile	yes	no
4	Cheyenne Mountain Complex/Tactical Warning – Attack Assessment	yes	yes
5	Combat Information Transport System	yes	no
6	Depot Maintenance Accounting and Production System	no	yes
7	Financial Information Resource System	yes	yes
8	Fuels Automated Management System Sustainment – Air Force	yes	no
9	Global Broadcast Service	yes	yes
10	Global Combat Support System- Air Force	yes	yes
11	High Frequency Global Communications System	no	yes
12	Integrated Logistics System – Supply	yes	yes
13	Integrated Maintenance Data System	yes	no
14	Integrated Strategic Planning and Analysis Network	yes	no
15	Mobility Command and Control	no	no
16	National Airspace System	yes	yes
17	Stock Control System	yes	yes

		Inconsistent Data Between:	
		IT Registry and ITMA CIRs	IT Registry Mission Assurance and Criticality Categories
Air Force Systems (cont'd)			
18	Theater Battle Management Core Systems	yes	yes
19	Theater Deployable Communications	no	yes
Defense Agency Systems			
Defense Finance and Accounting System			
1	Defense Cash Accountability System	yes	yes
2	Defense Civilian Pay System	yes	yes
3	Defense Departmental Reporting System	yes	yes
4	Defense Industrial Financial Management System	yes	yes
5	Defense Joint Military Pay System – Active and Reserve Components	yes	yes
6	Defense Working Capital Fund Accounting System	yes	yes
7	DFAS Corporate Database/Warehouse	no	yes
8	DFAS Electronic Business/Electronic Commerce	yes	no
9	E-Biz/Business Management Redesign	yes	yes
10	Electronic Document Management Program	no	no
11	Forward Compatible Payroll	yes	yes
12	General Accounting and Finance System	yes	yes
13	Marine Corps Total Force System	yes	yes
14	Mechanization of Contract Administration Services	yes	yes
15	Standard Accounting and Reporting System	yes	yes
16	Standard Accounting Budgeting and Reporting System	yes	yes
Defense Logistics Agency			
17	Business Systems Modernization – Energy	yes	yes
18	Distribution Standard System	no	yes
19	DLA Business Systems Modernization	no	yes
20	DoD Emall	yes	yes
U.S. Transportation Command			
21	Defense Enterprise Accounting and Management System	yes	no
22	Global Air Transportation Execution System	yes	yes
23	Global Decision Support System	no	no
24	Global Transportation Network 21	yes	yes

		Inconsistent Data Between:	
		IT Registry and ITMA CIRs	IT Registry Mission Assurance and Criticality Categories
Defense Agency Systems (cont'd)			
TRICARE Management Agency			
25	Defense Blood Standard System	yes	no
26	Defense Medical Human Resource System Internet	no	yes
27	Defense Medical Logistics Standard System	yes	no
28	Defense Occupational and Environmental Health Readiness System	no	yes
29	Enterprise Wide Scheduling and Registration	yes	yes
30	Executive Information/Decision Support	no	yes
31	Expense Assignment System IV	yes	yes
32	Military Computer-Based Patient Record	yes	yes
33	Theater Medical Information Program	no	yes
34	Third Party Outpatient Collection System	yes	no
35	TRANSCOM (Medical) Regulating and Command and Control Evacuation System	yes	no
36	TRICARE Online	yes	yes
Defense Human Resource Agency			
37	Defense Civilian Personnel Data System	yes	no
38	Defense Enrollment Eligibility Reporting System	yes	yes
39	Defense Integrated Military Human Resources System	yes	no
40	Protect Information – Common Access Card	yes	yes
Office of the Secretary of Defense			
41	Defense Travel System	yes	yes
42	High Performance Computing Modernization	yes	yes
43	Long-Range Planning and Analytical Support System	yes	yes
Defense Information Systems Agency			
44	Advanced Information Technology Services Joint Program Office	yes	no
45	Central Contractor Registration	no	no
46	Common Operating Environment	yes	yes
47	Defense Enterprise Computing Centers	no	no
48	Defense Information System Network	yes	no
49	Defense Message System	no	no
50	Defense Technical Information Center	yes	no
51	DoD Teleport	yes	no
52	Electronic Document Access	no	no

		Inconsistent Data Between:	
		IT Registry and ITMA CIRs	IT Registry Mission Assurance and Criticality Categories
Defense Agency Systems (cont'd)			
Defense Information Systems Agency (cont'd)			
53	Global Combat Support System	no	no
54	Global Command and Control System – Joint	yes	no
55	Global Exchange	no	yes
56	Joint Interoperability Test Command	yes	yes
57	Net Centric Enterprise Services	yes	no
58	White House Communications Agency	yes	no
59	Wide Area Workflow	yes	no
Defense Commissary Agency			
60	Point of Sales	yes	yes
61	Commissary Advanced Resale Transaction System	yes	yes
American Forces Information Services			
62	Network Support – Armed Forces Information Services	yes	no
Missile Defense Agency			
63	Computing Infrastructure	yes	yes
Defense Contract Management Agency			
64	Standard Procurement System	yes	yes

Appendix D. Mission Assurance Category and Mission Criticality Definitions

Mission Assurance Categories[1]	Mission Criticalities[2]
Mission Assurance Category I: Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a mission assurance category I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission assurance category I systems require the most stringent protection measures.	**Mission Critical**: A system in which the loss would cause the stoppage of warfighter operations or direct mission support of warfighter operations.
Mission Assurance Category II: Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness.	**Mission Essential:** A system that the acquiring Component Head determines basic and necessary for the accomplishment of the organizational mission.
Mission Assurance Category III: Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities.	**Mission Support:** A system that is neither mission critical nor mission essential.

[1]Defined in DoD Directive 8500.1, "Information Assurance," October 24, 2002.

[2]Defined in DoD Instruction 5000.2, "Operation of Defense Acquisition System," May 12, 2003 and Deputy CIO Memorandum, "Department of Defense Information Technology Registry Guidance for FY 2005," December 21, 2004.

Appendix E. Summary of Data Elements Reviewed

We reviewed 148 IT systems—32 Army, 33 Navy, 19 Air Force, and 64 Defense Agency—for consistent information between data elements in IT Registry reports and ITMA Capital Investment Reports. The following table summarizes, by data element and DoD Component, the 148 systems reviewed.

			Army	Navy	Air Force	Defense Agencies	Totals
1	Security Control Test Date	Inconsistent Systems	27	27	15	43	**112**
		Percent	84.4	81.8	78.9	67.2	**75.7***
2	Accreditation Date	Inconsistent Systems	12	12	8	17	**49**
		Percent	37.5	36.4	42.1	26.6	**33.1***
3	Accreditation Status	Inconsistent Systems	5	6	5	3	**19**
		Percent	15.6	18.2	26.3	14.1	**12.8***
4	Accreditation Method	Inconsistent Systems	2	2	4	4	**12**
		Percent	6.3	6.1	21.1	6.3	**8.1***
5	Accreditation Required	Inconsistent Systems	1	2	2	1	**6**
		Percent	3.2	6.1	10.5	1.6	**4.1***
6	System Security Authorization Agreement Status	Inconsistent Systems	4	8	2	2	**16**
		Percent	12.5	24.2	10.5	3.1	**10.8***
7	Risk Management Plan	Inconsistent Systems	5	3	2	6	**16**
		Percent	15.6	9.1	10.5	9.4	**10.8***
8	Security Plan	Inconsistent Systems	5	5	2	4	**16**
		Percent	15.6	15.2	10.5	6.3	**10.8***
9	Security Incident Response Plan	Inconsistent Systems	5	3	2	5	**15**
		Percent	15.6	9.1	10.5	7.8	**10.1***

*This the percent between the total inconsistent systems and the total systems reviewed.

Appendix F. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director, Defense Business Transformation Agency
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
Assistant Secretary of Defense for Health Affairs/Chief Information Officer
Assistant Secretary of Defense for Intelligence Oversight/Chief Information Officer
Chief Information Officer, Office of the Secretary of Defense
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff
Chief Information Officer, Joint Staff

Department of the Army

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

Department of the Navy

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

Department of the Air Force

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

Unified Commands

Chief Information Officer, U.S. Northern Command
Chief Information Officer, U.S. Southern Command
Chief Information Officer, U.S. Joint Forces Command
Chief Information Officer, U.S. Pacific Command
Chief Information Officer, U.S. European Command
Chief Information Officer, U.S. Central Command
Chief Information Officer, U.S. Transportation Command
Chief Information Officer, U.S. Special Operations Command
Chief Information Officer, U.S. Strategic Command

Other Defense Organizations

Director, Defense Finance and Accounting Service
Director, Defense Information Systems Agency
Chief Information Officer, American Forces Information Service
Chief Information Officer, Defense Advanced Research Projects Agency
Chief Information Officer, Defense Contract Audit Agency
Chief Information Officer, Defense Contract Management Agency
Chief Information Officer, Defense Commissary Agency
Chief Information Officer, Defense Finance and Accounting Agency
Chief Information Officer, Defense Human Resource Activity
Chief Information Officer, Defense Information Systems Agency
Chief Information Officer, Defense Logistics Agency
Chief Information Officer, Department of Defense Education Activity
Chief Information Officer, Department of Defense Inspector General
Chief Information Officer, Defense Security Cooperation Agency
Chief Information Officer, Defense Security Service
Chief Information Officer, Defense Technical Information Center
Chief Information Officer, Defense Threat Reduction Agency
Chief Information Officer, DoD Test Resources Management Center
Chief Information Officer, Defense Technology Security Administration
Chief Information Officer, Missile Defense Agency
Chief Information Officer, Pentagon Force Protection Agency
Chief Information Officer, TRICARE Management Agency
Chief Information Officer, U.S. Mission North Atlantic Treaty Organization
Chief Information Officer, Washington Headquarters Service

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

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

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

December 2, 2005

MEMORANDUM FOR DEPUTY INSPECTOR GENERAL FOR AUDITING,
INSPECTOR GENERAL OF THE DEPARTMENT OF DEFENSE

SUBJECT: Draft Report on "Security Status for Systems Reported in DoD Information Technology Databases," (Project No. D2005-D000AL-0156)

Thank you for the opportunity to review the draft subject report. The attached document provides our position regarding the findings and recommendations contained within the report. We look forward to further coordination on this highly important topic. The DoD Chief Information Officer point of contact on this matter is Megen Davis, (703) 604-1489 ext. 140, Megen.Davis@osd.mil.

Priscilla E. Guthrie
Deputy Assistant Secretary of Defense
(Deputy CIO)

Attachment:
As Stated

cc:
DASD(Resources), OASD(NII)

Response to Office of Inspector General Draft Audit Report,
"Security Status for Systems Reported in DoD Information Technology Databases"
(Project No. D2005-D000AL-0156)

IG Recommendation 1: Immediately commence utilization of automatic data integrity controls on DoD-wide IT databases to preclude population of data elements with invalid entries as recommended by the IG in August 2002.

Response: **Concur**. Institutionalization of automatic data integrity controls for DoD-wide IT databases has been a consistent DoD CIO priority. The DoD CIO plans to establish the DoD IT Management Data Community of Interest (COI) with a kick-off meeting in December 2005. This COI will begin the process of building a Net-Centric capability for publishing and subscribing to all authoritative IT Management Data. When complete, the processes established by the COI will ensure that data elements across the department are populated by and traceable to the DoD authoritative.

IG Recommendation 2: Identify and impose penalties beginning in the first quarter of FY 2006 on DoD Component CIOs.

Response: **Nonconcur**. We nonconcur on imposing penalties on CIOs; however, we agree that we can put in place or strengthen existing mechanisms that will help enforce data integrity. The DoD CIO will address the issues identified below through our governance processes and mechanisms.

> **IG Recommendation 2.a: Identify and impose penalties beginning in the first quarter of FY 2006 on those DoD Component CIOs that did not implement sufficient controls to ensure that all common security data elements in the Information Technology Registry/DoD Information Technology Portfolio Repository (IT Registry/DITPR) and the Information Technology Management Application/Select and Native Programming Information Technology (ITMA/SNaP-IT) databases are the same.**
>
> **Response**: **Concur**. Forthcoming DoD Federal Information Security Management Act (FISMA) Guidance, DITPR Guidance, and IT Budget Guidance will reemphasize that each Component CIO is responsible for ensuring that all common security data elements in the IT Registry/DITPR and the ITMA/SNaP-IT databases are the same. In addition, as mentioned in the response to Recommendation 1 above, the IT Management Data COI will be working to implement a net-centric solution that will ensure authoritative data is provided for internal and external requests for information.

IG Recommendation 2.b: Identify and impose penalties beginning in the first quarter of FY 2006 on those DoD Component CIOs that did not reconcile the security data elements in the IT Registry/DITPR and the ITMA/SNaP-IT databases at least quarterly to ensure that they are the same.

Response: Partially Concur. The IT Budget data, collected in SNaP-IT, is collected twice annually (September and February) and quarterly reconciliation would be inefficient and provide no benefit. However, the DoD will establish an automated annual security data elements reconciliation process that will be institutionalized through the databases' Configuration Control Boards and the results and status of corrective actions reported to the DoD CIO and CIO Executive Board. Component CIO's that have mismatched security data will be requested to take immediate corrective action.

IG Recommendation 2.c: Identify and impose penalties beginning in the first quarter of FY 2006 on those DoD Component CIOs that did not populate all required data elements in the IT Registry/DITPR and the ITMA/SNaP-IT databases.

Response: Concur. The DoD CIO is in the process of developing annual DITPR Guidance. This guidance will identify mandatory data elements that must be populated in DITPR. Effective immediately with the publication of this Guidance, expected to be issued in December 2005, all DITPR systems will have 90 days to comply. If uncorrected after 90 days, the system will be deleted from DITPR and placed in a holding area and identified to the DoD CIO. We note that the OASD(NII) Resources Directorate is in the process of identifying those data elements that are required in SNaP-IT and issuing those requirements to the SNaP-IT development team. The application will be used to ensure required data is completed. The majority of SNaP-IT data elements are passed to DoD by OMB in an XML Schema. All elements required by the OMB XML Schema are currently required elements within SNaP-IT.

IG Recommendation 3: Include the requirement in all future DITPR guidance that DoD Components explicitly certify in writing that the information in the DITPR is complete and correct.

Response: Concur. In response to the Fiscal Year 2005 National Defense Authorization Act, the Department recently issued a Concept of Operations for Investment Review Boards. The document provides the necessary detail regarding governance, roles, responsibilities, processes, controls, and reporting requirements to ensure that component

IT investments are visible to the highest levels of the Department and are in compliance with Mission Area guidance and recommendations.

IG Recommendation 4: Review the IT Registry/DITPR certifications to ensure that DoD Components are submitting required certification. Identify and impose sanctions beginning in the first quarter FY 2006 on those DoD Components that do not:

a. Submit a certification prior to the due date;
b. Include a date on the certification statement; and
c. Explicitly state that the information in the IT Registry/DITPR is complete and correct.

Response: Concur. Those DoD CIO's who do not (a) submit a certification prior to the due date; (b) include a date on the certification statement; and (3) explicitly state that the information in the IT Registry/DITPR is complete and correct, will be identified to the DoD CIO and required to explain their inactions to the DoD CIO Executive Board.

IG Recommendation 5: Require DoD Components CIOs in FY 2006 and beyond to submit the IT Registry/DITPR certifications prior to submitting the DoD FISMA Report to OMB.

Response: Concur. Certifications will annually be required by the first of September.

IG Recommendation 6: Advise OMB and Congress that DoD does not have viable internal controls over the accuracy of data it is reporting concerning the security of its IT systems and investments and caveat all reports based on data drawn from unreliable databases, such as the IT Registry/DITPR and the ITMA/SNaP-IT until such time as demonstrably effective internal controls have been in place for at least one full year reporting cycle.

Response: Nonconcur. The FY07 Exhibit 300 review process has greatly improved the data quality of the security data submissions in the Exhibit 300s. The resources managers were briefed on the FY06 Exhibit 300 DoD OIG finding in a June 2005 Exhibit 300 meeting. In addition, all Component FISMA Information Assurance (IA) officials were briefed to review both databases for consistency for the FY07 submissions.

IG Recommendation 7: Develop internal control mechanisms other than Component CIO and CFO certifications, report the discrepancies between DoD databases as a material control weakness, and develop a Plan of Action and Milestones to track and correct conditions.

Response to Office of Inspector General Draft Audit Report,
"Security Status for Systems Reported in DoD Information Technology Databases"
(Project No. D2005-D000AL-0156)

Response: See below.

IG Recommendation 7.a: Develop internal control mechanisms other than Component Chief Information Officer and Chief Financial Officer certifications.

Response: Concur. The ITMA application is being re-hosted as a component of the Select and Native Programming database owned and operated by the Director, Program Analysis and Evaluation (PA&E). Once re-hosted, the DASD-Resources and PA&E will work toward integrating the IT Budget with the overall DoD budget. Once integrated, adequate management controls should be available to ensure the IT Budget is aligned with the overall DoD budget and the Statement of Compliance can be eliminated.

IG Recommendation 7.b: Report the discrepancies between DoD databases as a material control weakness.

Response: Nonconcur. We do not agree that inconsistencies between our databases represent a material weakness. We have thoroughly examined our database requirements and identified areas where we can strengthen the integration of or interface between our databases. Also, the merger of the IT Registry and the DITPR will allow for better data integration and integrity.

IG Recommendation 7.c: Develop a Plan of Action and Milestones to track and correct conditions.

Response: Nonconcur. As indicated above, DoD is actively taking steps to ensure that our databases contain consistent and accurate data.

IG Recommendation 8: Adopt NIST FIPS Publication 199 to categorize information and information systems and revise the IT Registry/DITPR and the ITMA/SNaP-IT data elements accordingly.

Response: Nonconcur. While they are in a sense equivalent because they achieve the same ends, there are fundamental differences between FIPS 199 Potential Impact Definitions and DoD Mission Assurance Categories and Confidentiality Requirements that DoD uses to categorize information systems. The differences stem primarily from the facts that the former are focused on the potential impact to specific organizational operations, assets, and individuals while the latter have a focus that concerns itself primarily with potential impact to operational readiness and mission effectiveness of

deployed and contingency military forces and not just the impact to the organization operating the system. Additionally, FIPS 199 is not applicable to the National Security Systems (NSS) that make up the vast majority of DoD information systems so it does not address classified information at all. FISMA requires that agencies not following a FIPS have a more stringent standard.

DoD IA policy, primarily promulgated in DoDI 8500.2, is more stringent than FIPS 199 for confidentiality because the FIPS 199 definitions for MODERATE and HIGH impact equate to classified information for DoD and that requires application of the more stringent IA controls required for classified systems, including such things as Type 1 cryptography and SECRET or higher clearances for access. Further, for DoD, determining "information type" according to FIPS 199 for confidentiality protection of unclassified information has absolutely no value. It makes no difference if it is law enforcement, administrative, financial, privacy, procurement sensitive, medical, etc., our policies assume that all unclassified DoD information not specifically cleared for public release is "DoD Sensitive" information, and it is protected accordingly.

Regarding integrity, DoD only has two levels. MAC I and II systems must ensure absolute integrity of data and information. For MAC III systems the loss of integrity can be overcome without significant impact to mission effectiveness. Information "type" is a consideration (e.g., the integrity of financial data is generally more important than that of most administrative information) but one does not need to follow the FIPS 199 "generalized format" to determine which level of integrity is required. Since the Department cannot tolerate the "serious" adverse effects associated with the FIPS 199 MODERATE impact for integrity the DoD standard is more stringent because it requires absolute integrity at both the FIPS 199 MODERATE and HIGH impact levels.

Regarding availability, DoD has three levels that are expressed in terms of the time a system is not available (i.e., none, minutes to hours, hours-to-days) but they can be compared to the three impact levels in FIPS 199 and appear essentially equivalent. So DoD, at least meets the standard for availability.

Finally, the protection afforded by confidentiality controls to classified systems also enhances integrity and availability by restricting both physical and logical access to cleared individuals with a need-to-know and imposing other rules and restrictions associated with the handling and treatment of classified information. So, all DoD classified systems, whether MAC I, MACII, or MAC III, meet these more stringent requirements. Also, all security related data elements within ITMA/SNaP-IT are in accordance with OMB A-11, Sections 300 and 53.

Response to Office of Inspector General Draft Audit Report,
"Security Status for Systems Reported in DoD Information Technology Databases"
(Project No. D2005-D000AL-0156)

Additional Comments on Report Findings:

Technical Comments:

Third recommendation misnumbered as Recommendation "2."

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
Karen J. Lamar
Robert R. Johnson
Rebecca S. Courtade