Report No. D-2008-047 February 5, 2008

Inspector General
United States Department of Defense

Contingency Planning for DoD Mission-Critical Information Systems

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 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 the Office of the Deputy Inspector General for Auditing at (703) 604-9142 (DSN 664-9142) or fax (703) 604-8932. Ideas and requests can also be mailed to:

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

DEPARTMENT OF DEFENSE
hotline

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

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

Acronyms

ASD(NII)/CIO	Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
CIO	Chief Information Officer
COOP	Continuity of Operations Plan
DITPR	DoD Information Technology Portfolio Repository
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
FISMA	Federal Information Security Management Act
IG	Inspector General
MAC	Mission Assurance Category
ODO	Other Defense Organizations

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

February 5, 2008

MEMORANDUM FOR DISTRIBUTION

SUBJECT: Report on Contingency Planning for DoD Mission-Critical Information Systems (Report No. D-2008-047)

We are providing this report for review and comment. The U.S. Strategic Command and the Business Transformation Agency did not respond to the draft report. When preparing the final report, we considered management comments from the Assistant Secretary of Defense for Networks and Information Integration; the Departments of the Army, Navy, and Air Force; the U.S. Transportation Command; the Defense Contract Management Agency; the Defense Information Systems Agency; the Defense Logistics Agency; the Defense Threat Reduction Agency; the Missile Defense Agency; and TRICARE Management Activity.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Defense Information Systems Agency comments were responsive with the exception of Recommendation 2.e. We request that the Department of the Air Force, U.S. Strategic Command, U.S. Transportation Command, Business Transformation Agency, Defense Logistics Agency, Missile Defense Agency, and TRICARE Management Activity provide comments on the final report for Recommendations 2.a. through 2.j. See the Management Comments Required table at the end of the finding section for the specific comments required.

We also request that comments be provided on the final report by the Assistant Secretary of Defense for Networks and Information Integration for Recommendations 1.b., 1.d., 2.a., 2.b., 2.d., 2.e., 2.f., 2.g., 2.h., and 2.i.; the Army for Recommendations 2.c., 2.g., 2.h., and 2.i.; the Navy for Recommendations 2.a., 2.b., 2.c., 2.d., 2.e. 2.g., 2.h., 2.i., and 2.j.; the Defense Contract Management Agency for Recommendations 2.b., 2.c., 2.d., 2.e., 2.f., 2.g., and 2.h.; the Defense Information Systems Agency for Recommendation 2.e.; and the Defense Threat Reduction Agency for Recommendations 2.a., 2.b., 2.c., 2.d., 2.e., 2.f., 2.g., and 2.j. We request that management provide comments by March 5, 2008.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudROS@dodig.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. Kimberley A. Caprio at (703) 604-9202 (DSN 664-9202) or Ms. Karen J. Goff at (703) 604-9005 (DSN 664-9005). See Appendix D for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Robert F. Prinzbach II
Acting Assistant Inspector General
Readiness and Operations Support

DISTRIBUTION:

UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS AND INFORMATION INTEGRATION /CHIEF INFORMATION OFFICER
COMMANDER, U.S. STRATEGIC COMMAND
COMMANDER, U.S. TRANSPORTATION COMMAND
ASSISTANT SECRETARY OF THE AIR FORCE (FINANCIAL MANAGEMENT AND COMPTROLLER)
ASSISTANT SECRETARY (WARFIGHTING INTEGRATION) AND CHIEF INFORMATION OFFICER, DEPARTMENT OF THE AIR FORCE
DIRECTOR, BUSINESS TRANSFORMATION AGENCY
DIRECTOR, DEFENSE CONTRACT MANAGEMENT AGENCY
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENY
DIRECTOR, DEFENSE THREAT REDUCTION AGENCY
DIRECTOR, MISSILE DEFENSE AGENCY
DIRECTOR, TRICARE MANAGEMENT ACTIVITY
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE ARMY
CHIEF INFORMATION OFFICER, DEPARTMENT OF THE NAVY
DEPUTY CHIEF INFORMATION OFFICER, U.S. MARINE CORPS
CHIEF INFORMATION OFFICER, U.S. STRATEGIC COMMAND
CHIEF INFORMATION OFFICER, U.S. TRANSPORTATION COMMAND
CHIEF INFORMATION OFFICER, DEFENSE CONTRACT MANAGEMENT AGENCY
CHIEF INFORMATION OFFICER, DEFENSE INFORMATION SYSTEMS AGENCY
CHIEF INFORMATION OFFICER, DEFENSE LOGISTICS AGENY
CHIEF INFORMATION OFFICER, DEFENSE THREAT REDUCTION AGENCY
CHIEF INFORMATION OFFICER, MISSILE DEFENSE AGENCY
CHIEF INFORMATION OFFICER, TRICARE MANAGEMENT ACTIVITY
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

Department of Defense Office of Inspector General

Report No. D-2008-047 **February 5, 2008**
(Project No. D2007-D000LB-0080.000)

Contingency Planning for DoD Mission-Critical Information Systems

Executive Summary

Who Should Read This Report and Why? DoD Component Chief Information Officers and system owners conducting contingency planning for DoD information systems—in particular, DoD officials responsible for developing, testing, and approving system contingency plans—should read this report to properly plan and test their information systems before a contingent event. Also, DoD officials responsible for reporting contingency information to the Office of Management and Budget and Congress should read this report.

Background. Section 301, Public Law 107-347, Title III, "Federal Information Security Management Act of 2002," December 17, 2002, of the E-Government Act of 2002 requires each Federal agency to develop, document, and implement an agency-wide information security program. The Federal Information Security Management Act requires that Federal agency information security programs provide, among other things, plans and procedures for the continuity of operations for agency information systems to continue operations during a disruptive or catastrophic event. This is called contingency planning. DoD uses the DoD Information Technology Portfolio Repository (DITPR) as its primary information source for reporting on the security status of its DoD information systems for the Federal Information Security Management Act.

DITPR is the DoD authoritative repository of unclassified information for DoD information systems used to meet a variety of internal and external reporting requirements. Chief Information Officers of DoD Components are required to report in DITPR their inventory of information systems and must annually certify, in writing, that the Component's information in DITPR is complete and accurate. The system information in DITPR includes information on contingency planning, such as whether system owners developed and tested system contingency plans.

Contingency planning is the interim measure used to recover information technology services following an emergency or system disruption. Contingency planning is especially important for mission-critical systems. The loss of operations of mission-critical systems would cause the stoppage of warfighter operations. The Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer is required to develop and oversee contingency policies and planning for the stabilization and reconstruction of DoD operations.

On January 24, 2007, the date of the audit announcement, DoD reported in DITPR 436 mission-critical information technology systems requiring information assurance certification and accreditation. From the 436 systems, we statistically selected an audit sample of 240 systems for data analysis. We projected our results to all 436 DoD mission-critical information systems reported in DITPR as of January 24, 2007. See Appendix B for a list of the 240 mission-critical information systems in our sample.

Results. The information in DITPR on contingency planning is not reliable on the basis of sample results. We projected that, of 436 mission-critical information systems requiring

information assurance certification and accreditation, 264 systems (61 percent) lacked a contingency plan or their owners could not provide evidence of a plan, 358 systems (82 percent) had contingency plans that had not been tested or for which their owners could not provide evidence of testing, 410 systems (94 percent) had incorrect testing information reported in DITPR, and 37 systems (8 percent) had incorrect contingency plan information reported in DITPR. As a result, DoD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event. Further, DoD provided erroneous information to Congress and the Office of Management and Budget on whether DoD had contingency planning procedures in place and periodically tested the procedures necessary to recover the systems from an unforeseen, and possibly devastating, event. See the Finding section of the report for the detailed recommendations.

ASD(NII)/CIO did not implement management controls by establishing a comprehensive and overarching contingency planning policy. Further, DoD Component CIOs did not implement management controls to verify that system owners developed and tested system contingency plans as required or to support the assertions in their CIO Certification Memorandums about the completeness and accuracy of their information in DITPR.

Management Comments. The U.S. Strategic Command and the Business Transformation Agency did not respond to the draft report, issued on October 2, 2007. With the exception of Recommendations 1.c., 2.a., and 2.d. the Assistant Secretary of Defense for Networks and Information Integration concurred with the recommendations. The Departments of the Army and Navy concurred and the Defense Contract Management Agency partially concurred with the recommendations. Although the Defense Information Systems Agency comments did not state concurrence, the comments indicated concurrence. The Defense Threat Reduction Agency nonconcurred with Recommendation 2.c. and partially concurred with some of the recommendations.

The Air Force and the U.S. Transportation Command commented on the finding of the draft report; however, the comments did not indicate concurrence, proposed actions, or completion dates to the recommendations. The Defense Logistics Agency, Missile Defense Agency, and TRICARE Management Activity concurred with the recommendations; however, did not indicate proposed actions or completion dates. The U.S. Marine Corps provided unsolicited comments to the finding and Recommendation 2. and the Defense Threat Reduction Agency provided unsolicited comments to Recommendation 1.

Management Comments Required. We request that the U.S. Strategic Command and the Business Transformation Agency provide comments to the final report on Recommenda-tions 2.a. through 2.j. Further, we request that the Department of the Air Force, U.S. Transportation Command, Defense Logistics Agency, Missile Defense Agency, and TRICARE Management Activity provide comments on the final report regarding proposed actions and their completion dates for Recommendations 2.a. through 2.j.

We also request that comments on the final report be provided by the:

- Assistant Secretary of Defense for Networks and Information Integration—Recommendations 1.b., 1.d., 2.a., 2.b., 2.d., 2.e., 2.f., 2.g., 2.h., and 2.i.;
- Army—Recommendations 2.c., 2.g., 2.h., and 2.i.;
- Navy—Recommendations 2.a., 2.b., 2.c., 2.d., 2.e. 2.g., 2.h., 2.i., and 2.j.;

- Defense Contract Management Agency—Recommendations 2.b., 2.c., 2.d., 2.e., 2.f., 2.g., and 2.h.;

- Defense Information Systems Agency—Recommendation 2.e.; and

- Defense Threat Reduction Agency—Recommendations 2.a., 2.b., 2.c., 2.d., 2.e., 2.f., 2.g., and 2.j.

We request that management provide comments by March 5, 2008. See the Finding section of the report and Appendix C for a discussion of management comments and the Management Comments section of the report for the complete text of the comments.

Table of Contents

Executive Summary i

Background 1

Objectives 2

Review of Internal Controls 2

Finding

Contingency Planning for DoD Mission-Critical Information Systems 3

Appendixes

A. Scope and Methodology 37
Prior Coverage 40
B. DoD Mission-Critical Systems Sampled 41
C. Management Comments on the Finding, Unsolicited Comments on the Finding and Recommendations, and Audit Response 52
D. Report Distribution 55

Management Comments

Assistant Secretary of Defense for Networks and Information Integration 59
Department of the Army 68
Department of the Navy 77
Department of the Air Force 80
U.S. Transportation Command 81
Defense Contract Management Agency 83
Defense Information Systems Agency 87
Defense Logistics Agency 91
Defense Threat Reduction Agency 92
Missile Defense Agency 98
TRICARE Management Activity 99
U.S. Marine Corps 102

Background

Section 301, Public Law 107-347, Title III, "Federal Information Security Management Act of 2002," December 17, 2002, of the E-Government Act of 2002 requires that Federal agencies develop, document, and implement an agency-wide information security program. The Federal Information Security Management Act (FISMA) requires that Federal agency information security programs provide, among other things, plans and procedures for the continuity of operations for agency information systems. FISMA also requires that each Federal agency report annually to the Office of Management and Budget and Congress on the adequacy and effectiveness of its information security policies, procedures, and practices, which include contingency planning. DoD uses the DoD Information Technology Portfolio Repository (DITPR) as its primary source of information for FISMA reporting.

DoD Information Technology Portfolio Repository. DoD Chief Information Officer (CIO) Memorandum, "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SIPRNet IT Registry Annual Guidance for 2006," May 17, 2006 (FY 2006 DITPR Guidance), states that DITPR is the sole DoD authoritative repository of unclassified information for DoD information systems. DoD uses DITPR to meet a variety of internal and external reporting requirements, including FISMA reporting. The DoD Component CIOs are required to report in DITPR their inventory of information systems and must annually certify, in writing, that the Component's information in DITPR is complete and accurate. The system information in DITPR includes contingency planning information—specifically, whether system owners developed and tested system contingency plans.

Information is entered into DITPR by the Components using either batch uploads from their internal information technology systems or by working online in DITPR directly. Of the organizations reviewed, the Army, Navy, Air Force, Marine Corps, and TRICARE Management Activity update their DITPR information by batch upload. The remainder of the Components reviewed enter and edit their DITPR information online.

Contingency Planning. Contingency planning is the interim measure used to recover information technology services following an emergency or system disruption. Contingency planning is especially important for mission-critical systems. The loss of mission-critical system operations would cause the stoppage or direct mission support of warfighter operations. DoD Directive 5144.1, "Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/CIO)," May 2, 2005, requires that ASD(NII)/CIO develop and oversee contingency policies and planning for the stabilization and reconstruction of DoD operations. DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997,[1] requires that system owners prepare

[1] Subsequent to the audit, DoD Instruction 5200.40 was cancelled and replaced with DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007.

contingency plans as part of the information assurance certification and accreditation process of a system.

We queried DITPR on January 24, 2007, the date of our audit announcement, to identify the universe of DoD mission-critical information technology systems requiring information assurance certification and accreditation. The certification and accreditation process encompasses the actions taken by owners of a system to protect the system's information. Owners accomplish this by implementing information assurance controls designed to protect the availability, integrity, authentication, confidentiality, and non-repudiation of a system's information.

Our query resulted in a universe of 436 mission-critical information systems requiring information assurance certification and accreditation. The 436 systems included 110 Army, 97 Navy, 85 Air Force, 50 Marine Corps, and 94 Other Defense Organizations (ODO).[2] From a population of 436 systems, we statistically selected an audit sample of 240 systems. The audit sample consisted of 60 Army, 54 Navy, 50 Air Force, 26 Marine Corps and 50 ODO systems. We projected our results to the universe of 436 DoD mission-critical information systems reported in DITPR as of January 24, 2007. See Appendix B for the 240 systems sampled.

Objectives

Our overall audit objective was to assess the reliability of contingency planning data reported in DITPR for selected information systems. Specifically, we assessed system owners' compliance with reporting requirements for contingency planning information. See Appendix A for a discussion of the scope and methodology and prior coverage related to the objectives.

Review of Internal Controls

We identified internal control weaknesses for ASD(NII)/CIO as defined by DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. ASD(NII)/CIO did not establish a comprehensive and overarching contingency planning policy. Further, DoD Component CIOs did not implement management controls to verify that system owners developed and tested system contingency plans as required or to support the assertions in their CIO Certification Memorandums about the completeness and accuracy of their information in DITPR. Implementing Recommendations 1. and 2. will improve ASD(NII)/CIO and Component CIO reporting of contingency planning information in DITPR. We will provide a copy of the report to the senior official responsible for internal controls at ASD(NII)CIO in February 2008.

[2] An ODO is either a Defense agency or a combatant command.

Contingency Planning for DoD Mission-Critical Information Systems

The information in DITPR on contingency planning is not reliable on the basis of sample results. We projected that, of 436 mission-critical information systems requiring information assurance certification and accreditation:

- 264 systems (61 percent) lacked a contingency plan or their owners could not provide evidence of a plan;
- 358 systems[3] (82 percent) had contingency plans that had not been tested or for which their owners could not provide evidence of testing;
- 410 systems (94 percent) had incorrect testing information reported in DITPR; and
- 37 systems (8 percent) had incorrect contingency plan information reported in DITPR.

These security weaknesses occurred because ASD(NII)/CIO did not establish a comprehensive contingency planning policy. Additionally, the Component CIOs did not implement management controls to verify that system owners developed or tested system contingency plans. The Component CIOs also did not implement Component-level automated controls to ensure complete and accurate reporting in DITPR. As a result, DoD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event. Further, DoD provided erroneous information to Congress and the Office of Management and Budget on whether DoD had procedures in place and periodically tested the procedures necessary to recover the systems from an unforeseen, and possibly devastating, event.

Preparing Contingency Plans

DoD Instruction 5200.40 requires that system owners prepare contingency plans as part of the information assurance certification and accreditation process of a system. The certification and accreditation process encompasses the actions taken by owners of a system to protect the system's information. Owners accomplish this by implementing information assurance controls designed to protect the availability, integrity, authentication, confidentiality, and nonrepudiation of a system's information. On January 24, 2007, the date of the audit announcement, DoD reported in DITPR 436 mission-critical information

[3] The figure 358 was a result of sampling and computed independently. The figure does not reflect a total of the 97 Army, 86 Navy, 85 Air Force, 50 Marine Corps, and 39 ODO systems identified in this report whose system owners did not test or provide evidence of testing their system's contingency plan.

technology systems requiring information assurance certification and accreditation. Out of the 436 systems, we statistically selected 240 systems for data analysis. On the basis of sample results, we projected that owners of 264[4] of 436 mission-critical DoD systems did not develop or could not provide evidence of the systems contingency plan.

We requested that DoD Components provide us with the approved, signed copy of the system's contingency plan for the 240 systems sampled. When the Component did not provide a plan for the sampled systems, we stated that the system owner did not provide evidence of having developed a plan for that system. When system owners provided documentation, we reviewed the documentation to determine whether it met contingency plan requirements. See Appendix A for more on our methodology.

Army. On the basis of sample results, we projected that owners for 57 of the Army's 110 mission-critical systems (52 percent) did not develop or could not provide evidence of a contingency plan. Army system owners provided various reasons for not developing or providing system plans. For example, two system owners stated that because the system was a mission support system it did not require a plan. However, according to DITSCAP, system owners are required to develop a system contingency plan regardless of the system's mission criticality. Another system owner who could not provide a copy of the system's plan planned to delete the system from DITPR; however, the owner reported in DITPR that a plan had been developed for the system. Another system owner planned to transfer the system to another DoD Component and delete the system from DITPR. The owner, however, could not provide a copy of the system's plan and, at the time of our review, continued to report the system as owned by the Army.

Army system owners also provided documents that did not meet contingency plan requirements. For example, system owners provided continuity of operations plans (COOPs) that made no mention of the system under review. A COOP restores mission and organizational operations, which may not always include the restoration of an information system. One system owner provided a COOP stating that its purpose was to restore command operations. The COOP, however, did not include contingency planning for the information system sampled. Three system owners provided documents stating that unit commanders were responsible for developing their systems' contingency plans. However, Army officials could not provide the contingency plans for the three systems sampled. Further, the documents did not provide unit commanders with instructions for developing the system plans. In addition, two system owners provided contingency plans prepared specifically for the year 2000 conversion that did not identify procedures to recover the system from other disruptive events. The year 2000 conversion plans were more than 7 years old and did not state that the procedures identified in the plan were valid for the system's current environment.

Navy. On the basis of sample results, we projected that owners of 68 of the Navy's 97 mission-critical information systems (70 percent) did not develop or could not provide evidence of a contingency plan. System owners provided various reasons for not providing system plans. For example, one system owner

[4] The 264 systems include 57 Army, 68 Navy, 68 Air Force, 50 Marine Corps, and 21 ODO systems.

said the system was terminated. Another system owner who could not provide a contingency plan removed the system from DITPR because it was a network, not an information technology system. However, DITSCAP requires that system owners certify and accredit networks, as well as information systems. Therefore, the system owner should have prepared a contingency plan for the network.

Navy system owners provided documents that did not meet contingency plan requirements. For example, system owners provided technical manuals and headquarters COOPs. The documents, however, did not include contingency plans specific to their information system to recover from a disruptive event or emergency. System owners also provided one-page documents stating that the contingency plan was the responsibility of the information assurance manager. Navy officials, however, could not provide contingency plans for those systems. Further, the one-page documents did not provide guidance to the information assurance managers on how to recover the system from a disruptive event.

Air Force. On the basis of sample results, we projected that owners of 68 of the Air Force's 85 mission-critical information systems (80 percent) did not develop or could not provide evidence of a contingency plan. System owners provided documents that did not meet contingency plan requirements. One system owner provided task cards rather than a contingency plan. Task cards provide personnel with procedures for the orderly evacuation of personnel in case of fire, natural disaster, bomb threat, or other emergency. The tasks cards did not discuss procedures for restoring an information system's operations after a disruptive event. Another system owner provided a risk management plan that did not identify a contingency plan for the information system. Lastly, one system owner provided the system's COOP, which stated that users should use it in conjunction with the system's contingency plan. The system owner, however, could not provide the contingency plan.

Marine Corps. On the basis of sample results, we projected that system owners for all of the Marine Corps' 50 mission-critical information systems (100 percent) did not develop or could not provide evidence of a contingency plan. System owners reported in DITPR for the 26 systems sampled that they had developed a contingency plan for the system. However, Marine Corps system owners provided one document for all 26 systems sampled—an appendix from the Marine Corps Logistics Command Security System Authorization Agreement—as evidence that they had prepared contingency plans for the 26 systems. Marine Corps system owners also provided a memorandum stating that the appendix covered contingency planning procedures for the 26 systems under review. The five-page appendix, however, did not mention the 26 systems or provide contingency planning procedures for the systems.

Other DoD Organizations. Based on our sample results, we projected that owners of 21 of 94 ODO mission-critical information systems (22 percent) did not develop or could not provide evidence of a contingency plan. System owners stated that their systems did not have plans because the systems were, respectively, a pilot project, a network appliance, or a predeployment system. However, none of the reasons given by system owners precluded them from developing contingency plans. The owner of each system reported in DITPR that it required certification and accreditation; therefore, each system required a

contingency plan. Other system owners stated that the contractors operating their systems could not release the contingency plans to the Government because the plans contained proprietary information. The Component CIO should require that the contractors remove the proprietary information from the contingency plan and immediately provide the Government with a copy.

On the basis of our review of the contingency plans that did meet requirements, we found no consistency among the contingency plans prepared by system owners within DoD. Each plan contained varying degrees of information. For example, some plans contained system descriptions, system configurations schematics, and disaster recovery scenarios, while other plans did not. Additionally, some plans detailed the frequency of data backups, measures to protect critical software, and procedures for startup at alternate sites, while most plans did not.

Contingency Plan Testing

Despite evidence presented in the previous section of this report that system owners could not demonstrate they had developed a contingency plan for their system, owners still reported in DITPR on January 24, 2007, that, for 235 of the 240 systems sampled, they had tested the system's plan. System owners for the remaining five systems left blank the data field in DITPR that asks about contingency plan testing. We requested that system owners provide testing documents to support the date of the contingency plan test that owners reported in DITPR as of January 24, 2007.

On the basis of sample results, we projected that owners of 358 of 436 DoD mission-critical systems did not test or could not provide evidence that they tested system contingency plans. DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, requires that system owners test contingency plans based on the system's MAC (Mission Assurance Category). System owners are required to designate their system as a MAC I, II, or III. The MAC designates the importance of the information in relation to the achievement of DoD goals and objectives, particularly the warfighter's combat mission.

DoD Instruction 8500.2 requires that system owners test MAC I systems twice a year and MAC II and III systems once yearly. DoD CIO Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006 (FY 2006 FISMA Guidance), requires that system owners test the procedures in their contingency plans using tabletop[5] or functional[6] exercises and document the testing results. We based our review on the requirements in the FY 2006 FISMA Guidance because its deadline for updating DITPR, December 1, 2006, coincided

[5] Participants of a tabletop exercise walk through the procedures without any actual recovery operations occurring. Tabletop exercises are the most basic and least costly of the two types of exercises.

[6] Functional exercises include simulations and war gaming. Often, scripts are written for role players pretending to be external organization contacts. A functional exercise can include actual relocation to the alternate site.

most closely with the date on which we announced our audit and obtained our audit universe, January 24, 2007. Also, the DoD CIO did not issue the follow-on memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2007 (FY07)," May 21, 2007 (FY 2007 FISMA Guidance), until 4 months after we announced our audit and obtained the audit universe. Further, as part of the FY 2006 FISMA Guidance, the DoD CIO included supplemental information on the types of contingency plan exercises system owners should conduct and required owners to document the exercises. However, the DoD CIO omitted that supplemental information from the FY 2007 FISMA Guidance.

Army. On the basis of sample results, we projected that owners of 97 of the Army's 110 mission-critical information systems (88 percent) did not test or could not provide evidence that they tested a contingency plan. As evidence of testing, owners of systems in our sample provided memorandums for record, execution papers, and e-mail responses dated after our request for information. The FY 2006 FISMA Guidance requires that system owners maintain documents on contingency plan testing. We did not consider responses or documents prepared in response to our data request as evidence of contingency plan testing. Some system owners provided actual testing documents, but only two of the documents confirmed that testing was done on the date reported in DITPR. Other system owners provided a contingency plan that was dated after the testing date reported in DITPR.

Navy. On the basis of sample results, we projected that owners of 86 of the Navy's 97 mission-critical information systems (89 percent) did not test or could not provide evidence that they tested their systems' contingency plans. Owners of the Navy's systems we sampled entered a date in DITPR indicating when they last tested the contingency plan but did not always provide testing documents supporting that date. For example, some system owners did not provide any documentation, while others provided documentation that did not match the test date in DITPR. Specifically, system owners provided memorandums for record, prepared after the date of our data request, certifying that they tested the system contingency plan on the date reported in DITPR. We did not consider responses or documents prepared in response to our data request as evidence of contingency plan testing. We concluded that the system owners did not document the testing of the contingency plan as required by the FY 2006 FISMA Guidance.

In addition, Navy system owners provided COOP checklists identifying procedures that owners should include in their COOP plan. The COOP checklists were not specific to the systems under review. System owners also provided exercise and drill schedules and stated that they interviewed their information assurance officer to verify that exercises were completed. The COOP checklists and exercise and drill schedules did not document the actual completion of a contingency plan test. The COOP checklist also did not support that system owners conducted a contingency plan test on the date they reported in DITPR.

Further, few system owners documented testing results for their systems' contingency plans as required by the FY 2006 FISMA Guidance. Among system owners who did document testing results, most provided documents with dates

that did not match those reported in DITPR. In fact, some testing documents bore dates preceding the date of the contingency plan provided.

Air Force. On the basis of sample results, we projected that owners of all of the Air Force's 85 mission-critical information systems (100 percent) did not test or could not provide evidence of testing the contingency plan as required by DoD Instruction 8500.2 and the FY 2006 FISMA Guidance. We gave Air Force officials two opportunities to provide contingency plan testing documents for the systems in our sample. We concluded that system owners did not maintain testing documentation as required or perform testing of their systems' contingency plans.

Marine Corps. On the basis of sample results, we projected that owners of all of the Marine Corps' 50 mission-critical information systems (100 percent) did not test or could not provide evidence that they tested the systems' contingency plans. Responding to the question in DITPR about when they last tested their systems' contingency plans, owners of all but one sampled system reported the same date. These same owners, however, provided only one document—a COOP checklist for the Marine Corps Logistics Command—as evidence that they tested the contingency plans for the 26 systems sampled. The checklist provided steps for system owners to follow when developing a COOP plan but did not document the actual completion of the contingency plan test for any of the Marine Corps systems in our sample. Further, Marine Corps officials dated the COOP checklist after our documentation request. Therefore, the COOP checklist did not support the dates reported in DITPR for the 26 systems sampled.

Other DoD Organizations. On the basis of our sample results, we projected that owners of 39 of 94 mission-critical ODO information systems (42 percent) did not test or could not provide evidence that they tested their systems' contingency plans. For example, system owners provided documents indicating dates for planned testing but did not actually provide testing results. Other system owners provided test results for unidentified systems. Still other owners provided the approval memorandums granting their systems authority to operate. We did not consider these documents adequate support for testing the contingency plan. Finally, some owners responded that their systems did not have contingency plans.

In light of the significant deficiencies we identified in the testing of system contingency plans, the DoD CIO should issue supplemental guidance reinstating the contingency plan testing requirements identified in the FY 2006 FISMA Guidance. The DoD CIO removed clarifying guidance from the FY 2007 FISMA Guidance on the types of tests that system owners should conduct. The DoD CIO also omitted the requirement for system owners to document results of contingency plan tests. Further, the Component CIO should implement management controls to verify that system owners conduct recurring tests of system contingency plans.

Reporting on Contingency Planning in DITPR

According to the FY 2006 DITPR Guidance, DoD Components own and maintain the information reported in DITPR and are responsible for its completeness and accuracy. Based on sample results, we projected that owners of 410 of 436 DoD mission-critical information systems (94 percent) did not correctly report in DITPR whether they tested their systems' plans. Additionally, we projected that owners of 37 of the 436 information systems (8 percent) did not correctly report in DITPR whether they developed contingency plans for their systems.

Development of Contingency Plans. For all of the 240 mission-critical systems in our sample, system owners reported in DITPR that their systems required certification and accreditation. DITSCAP requires that system owners develop a system contingency plan as part of the certification and accreditation process.

When entering information in DITPR, system owners are required to enter "yes" or "no" in the data field that indicates whether they developed a contingency plan for their system. For the 240 certified and accredited mission-critical systems sampled, system owners should have developed a contingency plan for their system and responded "yes." We identified, however, that owners did not always respond "yes" in DITPR. On the basis of sample results, we projected that owners of 37 of 436 mission-critical systems (8 percent) belonging to the Army, Navy, Business Transformation Agency, Defense Information Systems Agency, and Defense Threat Reduction Agency reported "no," that they did not develop a plan, or left the data field blank. Navy system owners also answered "n/a."

Testing of Contingency Plans. On the basis of sample results, we projected that owners of 410 of 436 DoD mission-critical information systems (94 percent) could not support the contingency plan test date they reported in DITPR for their system or did not report a test date in DITPR. When the system owners did provide testing documents, the majority of the documents bore dates that did not match the date the owner reported in DITPR. The FY 2006 FISMA Guidance required that DoD Components make their first update in DITPR for FY 2007 by December 1, 2006.[7] The owners of several systems provided testing documentation dated after the date reported in DITPR but before December 1, 2006. That documentation indicated that system owners did not properly update the test date in DITPR.

DITPR information also indicates that some system owners had not tested their systems' contingency plans for more than 5 years. Specifically, owners of Navy and Air Force systems reported in DITPR that they last tested the systems' contingency plans in 2002. A Defense Logistics Agency system owner last reported testing the system's contingency plan in 2003.

Other DITPR Data. During our review of contingency planning documents, we identified other DITPR reporting problems. Specifically, we found that system owners reported the same systems twice in DITPR, that the documentation

[7] The FY 2006 FISMA Guidance established December 1, 2006, as the deadline for entering first-quarter FY 2007 updates in DITPR; we obtained our sample universe from DITPR on January 24, 2007.

owners provided did not match reporting for other DITPR data elements, and that system owners made unusual designations in DITPR.

Duplicate Reporting. In three cases, system owners from different Components reported the same system under different DITPR identification numbers. For example, system owners from the Army and the Navy reported the same system using DITPR identification numbers 3612 and 5021, respectively. System owners from the Navy and the U.S. Transportation Command reported the same system under DITPR identification numbers 4827 and 354, respectively. Finally, owners from the Army and U.S. Transportation Command reported the same system using DITPR identification numbers 3037 and 1352, respectively.

Conflicting or Missing DITPR Data. We also found instances when the documentation that system owners provided did not match other DITPR data fields or was incomplete. For instance, the owners of Army systems designated their systems as mission critical; however, the owner stated that the systems were mission support systems. Other Army owners left the testing data field blank.

Conflicts Between Data Entries and Documentation. Two Navy system owners reported their systems as MAC I; however, the documentation identified the system as MAC II. One of the two owners also reported in DITPR that their system was mission critical whereas the documentation they provided showed that the system was actually mission essential. Navy system owners also reported future dates in DITPR when answering the question about when they last tested the contingency plan. For example, we generated our audit sample on January 24, 2007; the DITPR information collected on that date showed that one Navy system owner reported having last tested the system's contingency plan in October 2007. Additionally, Navy system owners reported dates in DITPR to indicate when they last tested their systems' contingency plans, but also reported that they did not develop contingency plans for their systems.

During the review, Air Force officials did not provide any testing documentation on systems in our sample. Therefore, we projected that no Air Force system owners prepared or tested their systems' contingency plans or documented test results.

Unusual Designations. The FY 2006 FISMA Guidance states that system owners' designating their systems as mission critical and MAC III is unusual. The Guidance recommends that system owners review the designation combination closely before making such a designation in DITPR. The designation is unusual because a system owner is protecting a mission-critical system whose loss would stop warfighter operations with the minimum security required for any information system. System owners should protect their system at MAC III only when the consequences of the loss of its information can be tolerated or overcome without jeopardizing mission effectiveness or operational readiness. Owners of 17 Army, 5 Navy, 8 Air Force, 4 Marine Corps, and 5 ODO mission-critical systems designated their systems as MAC III. We could not find in the documentation any reasons given by owners for designating their systems as mission critical and MAC III.

Policy and Guidance

DoD Contingency Planning Policy. ASD(NII)/CIO did not establish a comprehensive policy for contingency planning. DoD contingency planning policy is fragmented and does not provide system owners with comprehensive policy for preparing contingency plans. DITSCAP requires system owners to prepare contingency plans but does not tell them how. DoD Instruction 8500.2 requires that system owners test certain aspects of the plan but does not identify the types of tests system owners must conduct or require that owners document results. Further, the DITPR Data Dictionary, which explains in detail what owners should report in each DITPR data field, is confusing. Specifically, the January 31, 2007, version of the DITPR Data Dictionary states that the "contingency test date" refers to the date a system owner last tested the system's contingency plan or COOP. In other words, the DITPR Data Dictionary uses the terms "contingency plan" and "COOP" interchangeably. The terms, however, have different meanings.

A contingency plan restores system operations, whereas a COOP restores mission and organizational operations. Because DITPR is the DoD repository for system information, we interpreted the DITPR Data Dictionary to require that Components enter the date the system's contingency plan was last tested. Because DITPR and the Data Dictionary use the terms interchangeably, we believe confusion exists among system owners about the difference between a contingency plan and a COOP. We base our conclusion on the documents owners provided to demonstrate that they had developed a plan for their systems. Specifically, numerous system owners provided the headquarters COOP in response to our data request rather than the system's contingency plan.

Guidance for Components on Contingency Planning. The Army, Navy, Air Force, U.S. Strategic Command, U.S. Transportation Command, Defense Contract Management Agency, Defense Threat Reduction Agency, Missile Defense Agency, and TRICARE Management Activity issued some form of guidance on contingency planning in the absence of an overarching DoD policy on contingency planning. The policy issued by the Army, Navy, Air Force, and the TRICARE Management Activity referred to the National Institute on Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, and recommended its use when preparing system contingency plans. Special Publication 800-34 identifies fundamental planning principles and practices to help personnel develop and maintain effective information technology contingency plans.

Despite the fact that some DoD Components recommended use of Special Publication 800-34, ASD(NII)/CIO has not formally mandated its use or established a comprehensive DoD contingency planning policy in accordance with DoD Directive 5144.1. ASD(NII)/CIO should either require that DoD Components implement Special Publication 800-34 or issue a comprehensive policy for contingency planning for DoD information systems. ASD(NII)/CIO should also develop a training program for DoD Components on contingency planning. The training program would ensure that system owners consistently prepare and test contingency plans.

DITPR Data Quality

DoD Component CIOs did not implement Component-level automated controls to help ensure complete and accurate reporting in DITPR. The DoD Components own the information systems reported in DITPR and are responsible to update and maintain their information system data reported in DITPR. According to the FY 2006 DITPR Guidance, the Components are responsible for the accuracy and completeness of their system data in DITPR and must implement automated controls that help ensure that system owners report complete, accurate, and up-to-date information in DITPR. The FY 2006 DITPR Guidance also required that the Component CIO certify in writing that automated controls were in place to help ensure DITPR data quality.

Military Departments. Army and Navy officials stated in their DITPR CIO Memorandums that they implemented automated controls. However, Army and Navy officials acknowledged that the automated controls were actually reports generated from their Service-level systems that officials manually reviewed to identify blank data fields. According to the officials, the manual reviews can determine only the completeness of their information, not its accuracy. Although manual reviews may be considered a control measure, manually reviewing a report to identify data anomalies is not an automated control. In September 2006, Air Force officials stated that they, too, implemented an automated tool; however, the tool was not in place at the time the Air Force CIO signed his DITPR CIO Certification Memorandum. Air Force officials also stated that the automated tool is now operational but that system owners are reluctant to use it.

Other Defense Organizations. Component CIOs for 7 of the 10 ODOs we sampled indicated in their annual CIO DITPR Certification Memorandums that they implemented automated controls. We found, however, that only the CIO from the TRICARE Management Activity had implemented automated controls as the remaining six CIOs did not implement the controls as certified in their memorandum. For example, a Defense Contract Management Agency official stated that the agency maintained a spreadsheet to track accreditation dates. Tracking accreditation dates only identifies when a system owner must re-accredit a system to operate and is not an example of an automated tool that would improve the quality of DITPR information. In addition, a U.S. Strategic Command official stated that he uses the Outlook calendar as a reminder to generate a monthly FISMA report from DIPTR. The official stated that he manually reviews the monthly report from DITPR to identify any inconsistencies.

ASD(NII)/CIO. ASD(NII)/CIO has taken steps to improve data quality of the information in DITPR. In August 2007, ASD(NII)/CIO officials responsible for managing DITPR included 16 built in checks, called data integrity rules, identifying when information in a data field is not logical. For example, one data integrity rule identifies when owners enter a future date in DITPR for when they last tested their contingency plan. Another rule identifies when owners enter a contingency plan test date but entered a “no” in the field asking whether they developed a plan for the system.

DITPR officials can also identify when owners leave certain data fields blank; however, officials stated that the challenge is to identify who is responsible for correcting the anomalies identified by these metrics. On September 7, 2007, ASD(NII)/CIO began requiring that Component CIOs complete a DoD Component Data Traceability Document, which describes the internal processes used by the Component to ensure that they inventoried all their information systems and that the data supplied in DITPR are accurate and taken from authoritative sources.[8] The Components must also document whether they independently validated their internal processes, the frequency of independent validation, and the validation results and remedial actions taken. DITPR officials plan to phase in the DoD Component Data Traceability Document requirement over the next 2 years. The new document will replace the DITPR CIO Certification Memorandums as long as Components update the traceability document annually.

Although DITPR provides automated controls to identify blank and illogical data, the DoD Components supply the information reported in DITPR and must provide accurate and complete information. To help improve DITPR data quality, ASD(NII)/CIO required in the FY 2006 DITPR Guidance that Component CIOs implement automated controls and certify that the system information reported to DoD in DITPR is complete and accurate. However, the DoD Components in our sample often did not implement such controls and continue to supply incorrect and inaccurate information in DITPR as identified in this audit report. Further, the FY 2006 DITPR Guidance did not provide DoD Components with a definition of an automated control or specify the types of automated controls that the Components should implement.

In view of the contingency planning reporting problems identified in this report, the DITPR Component CIO Memorandums currently provide no assurance as to the completeness and accuracy of information in DITPR. The new DoD Component Data Traceability Document will require Component CIOs to record their DITPR information processes and may identify ways to improve the quality of data in DITPR. Until the DoD Component Data Traceability Document is fully implemented across DoD, Component CIOs should closely review their DITPR CIO Certification Memorandums to ensure that the information is accurate. The Component CIOs should closely review the basis of their assertions on the accuracy and completeness of their information in DITPR and interview information assurance professionals to validate such assertions. The Component CIOs should also sanction system owners that continue to report inaccurate and incomplete information in DITPR. Finally, ASD(NII)/CIO should include caveats in reports drawn from DITPR stating that the information is not accurate or complete and should not be relied on for management and budgetary decisions.

[8] The DoD CIO updated the FY 2006 DITPR Guidance by issuing "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008," September 6, 2007.

Management Controls

We projected that owners of 264 out of 436 DoD mission-critical information systems (61 percent) did not develop or could not provide evidence of a contingency plan for their system. The contingency plans that system owners provided varied in content and in degree of completion: some were still in draft, and most were not approved. Additionally, we projected that owners of 358 out of 436 mission-critical information systems (82 percent) did not test or could not provide evidence of testing. Our sample results are evidence that the Component CIOs did not implement management controls to ensure that owners complied with contingency planning requirements. The Component CIOs should verify that system owners are developing viable contingency plans, that plans are approved, and that plans are tested under realistic and current conditions.

In light of the significant security weaknesses identified in this audit report—that owners of a projected 61 percent of DoD mission-critical information systems did not develop or could not provide evidence of a system's contingency plans and that 82 percent did not test plans as required—DoD Component CIOs should prepare Component-level Plans of Action and Milestones. The FY 2006 FISMA Guidance requires that Component CIOs and system owners develop, implement, and manage Plans of Action and Milestones for programs and systems they operate and control. A Plan of Action and Milestones is a management tool that documents system security weaknesses that owners must remediate and identifies the actions and milestones necessary for mitigating security weaknesses. According to the FY 2006 FISMA Guidance, a system owner should also prepare Plans of Action and Milestones when information technology security weaknesses are identified during a review. System owners should prepare a Plan of Action and Milestones to remediate the contingency planning weaknesses identified in Appendix B.

Conclusions

DoD mission-critical systems may not be able to sustain warfighter operations during a disruptive or catastrophic event without the development and testing of system contingency plans. The permanent loss of a mission-critical system would cause the stoppage of warfighter operations. Until ASD(NII)/DoD CIO issues a comprehensive DoD contingency planning policy, ASD(NII)/CIO should mandate that the DoD Components follow Special Publication 800-34 when developing system contingency plans. The DoD Component CIOs should implement management controls to verify that system owners reporting in DITPR, particularly on mission-critical systems, are developing system contingency plans. Similarly, the Component CIOs should implement controls to ensure that system owners are conducting recurring tests of the systems plans.

DoD provided erroneous information to Congress and the Office of Management and Budget on whether DoD had procedures in place and periodically tested the procedures necessary to recover the systems from an unforeseen event. DITPR is the only means for DoD to report the security status of its information technology

systems to the Office of Management and Budget and Congress and is being used to compile reports for FISMA, as well as for other congressional reporting requirements. The inaccurate and incomplete information in DITPR continues to diminish the usefulness of the database for management oversight by DoD, the Office of Management and Budget, and Congress. Unless DoD implements effective internal quality controls over Component-supplied information in DITPR, DoD reporting on the security status of its information systems continues to be flawed and should not be relied on.

Management Comments on the Finding, Unsolicited Comments on the Finding and Recommendations, and Audit Response

The Air Force, U.S. Transportation Command, and the Defense Contract Management Agency provided comments on the finding section of the report. Although not required to comment, the Marine Corps also commented on the finding and the Defense Threat Reduction Agency commented on Recommendation 1. Summaries of management comments on the finding, unsolicited comments on the finding and recommendations, and our audit response are in Appendix C.

Recommendations, Management Comments, and Audit Response

1. We recommend that the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer:

a. Require DoD Components to use the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, when developing and testing DoD contingency plans, or issue a comprehensive DoD contingency planning policy.

Management Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that the DoD CIO will recommend that Special Publication 800-34 be used as a guide when preparing system contingency plans.

Audit Response. The Deputy Assistant Secretary of Defense for Information and Identity Assurance comments were responsive, and no further comments are required.

b. Inform the Office of Management and Budget and Congress that DoD does not have internal controls over the accuracy of data on the security of its information technology systems, and include a caveat to that effect in all reports based on data drawn from the DoD Information Technology

Portfolio Repository until demonstrably effective internal controls have been in place for at least 1 full year.

Management Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that future reports generated using DIPTR as the principal source will include a caveat indicating that some DITPR data should be used with caution.

Audit Response. The Deputy Assistant Secretary of Defense for Information and Identity Assurance comments were nonresponsive. The Deputy Assistant Secretary of Defense for Information and Identity Assurance did not indicate whether ASD(NII)/CIO would inform the Office of Management and Budget and Congress that DoD does not have internal controls over the accuracy of data on the security of its information technology systems. Additionally, the Deputy's response to include a "caution" on DITPR data reports is ambiguous. Therefore, we request that ASD(NII)/CIO inform the Office of Management and Budget and Congress that DoD does not have internal controls over the accuracy of data on the security of its information technology systems. We also request that ASD(NII)/CIO provide additional comments on the final report identifying the specific language that will be used in reports generated from DITPR to alert users that the information in the report is not reliable.

c. Immediately issue a supplement to the DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) for Fiscal Year 2007 (FY07)," May 21, 2007, and all continuations of the guidance, that contains the information on testing contingency plans that was included in the supplemental section of the DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006.

Management Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, partially concurred, stating that since the FY 2007 FISMA reporting is complete, a supplement to that guidance would not be useful. The Deputy for Information and Identity Assurance agreed, however, to include additional guidance on contingency planning and testing in the FY 2008 FISMA Guidance, which will be issued in the first quarter of 2008.

Audit Response. The Deputy Assistant Secretary of Defense for Information and Identity Assurance comments were responsive, and no further comments are required.

d. Immediately issue a supplement to the DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008," September 6, 2007, and all continuations of the guidance, that:

(1) Defines an automated control and specifies the types of data integrity rules DoD Components must implement to ensure they enter complete, accurate, and authoritative data in the DoD Information Technology Portfolio Repository.

(2) Clarifies the difference between a contingency plan and a continuity of operations plan.

(3) Removes references to continuity of operations plans in the "contingency plan" and "contingency plan last exercised" data fields in the DoD Information Technology Portfolio Repository and the DoD Information Technology Portfolio Repository Data Dictionary.

Management Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that a software release in October 2007 included enhancements to DITPR data quality. The Deputy for Information and Identity Assurance stated that additional changes to implement automated application controls will be introduced in subsequent releases. The Deputy for Information and Identity Assurance also stated that the DoD CIO will supplement current DITPR guidance to clarify differences between contingency planning and continuity of operations planning.

Audit Response. The Deputy Assistant Secretary of Defense for Information and Identity Assurance comments were partially responsive. We request that ASD(NII)/CIO provide comments on the final report identifying the specific application controls that will be introduced into DITPR and the dates by which each control will be implemented.

e. Implement a training program in contingency planning for DoD Component officials who develop, test, and approve contingency plans for information systems.

Management Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred, stating that DoD will add guidance on DoD contingency planning to the information technology information assurance training program managed and operated by the Defense Information Systems Agency.

Audit Response. The Deputy Assistant Secretary of Defense for Information and Identity Assurance comments were responsive, and no further comments are required.

2. We recommend that the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer; the Director, Business Transformation Agency; and the Chief Information Officers for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the Defense Contract Management Agency, the Defense Information Systems Agency, the Defense Logistics Agency, the Defense Threat Reduction Agency, the Missile Defense Agency, and the TRICARE Management Activity:

a. Require that system owners develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, nonconcurred, stated that DoD is using the interim DoD Information Assurance Certification and Accreditation Process guidance instead of DoD Instruction 5200.40. However, the Deputy for Information and Identity Assurance stated that additional guidance will be provided recommending that Special Publication 800-34 be used as a guide when preparing contingency plans.

Audit Response. The Deputy Assistant Secretary of Defense for Information and Identity Assurance comments were partially responsive. Although ASD(NII)/CIO formally issued DoD Instruction 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," on November 28, 2007, the Instruction does not require that DoD Components implement information assurance policies and procedures issued by the National Institute of Standards and Technology as required by FISMA. ASD(NII)/CIO agreed in comments on this report to recommend that DoD Components use the National Institute of Standards and Technology Special Publication 800-34 as a guide when preparing system contingency plans, but did not indicate the planned date for issuing the supplemental guidance. Therefore, we request that ASD(NII)/CIO provide comments on the final report identifying a completion date for issuing the guidance requiring DoD Components to use Special Publication 800-34 when preparing system contingency plans.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army published Department of the Army Pamphlet 25-1-2, "Information Technology Contingency Planning," November 16, 2006. The Acting CIO stated that the Pamphlet implements DoD and Federal policy and was based on Special Publication 800-34.

Audit Response. The Army comments were responsive, and no further comments are required.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred, stating that the Navy CIO will issue specific guidance on this recommendation after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report identifying a completion date for issuing guidance requiring that system owners develop plans in accordance with Special Publication 800-34.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that

DoD CIO Memorandum, "Interim Department of Defense (DoD) Information Assurance Certification and Accreditation Process Guidance," July 6, 2006, instructed all DoD personnel to disregard DoD Instruction 5200.40 and comply with the requirements of draft DoD Instruction 8510.bb, "The DoD Information Assurance Certification and Accreditation Process (DIACAP)."

Audit Response. Although the Defense Contract Management Agency partially concurred, we considered the comments responsive, and no further comments are required.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that the agency uses the annual DoD FISMA Guidance, which requires systems to have a contingency plan that is developed and tested in accordance with DoD Instruction 8500.2.

Audit Response. The CIO, Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency partially concurred, stating that DITSCAP does not describe how to write or test a contingency plan, nor does its replacement, the DoD Information Assurance Certification and Accreditation Process. The CIO stated that while there is no current DoD policy that describes how to develop and test a contingency plan, Special Publication 800-34 provides a detailed description for writing a plan, explains how contingency planning fits into the system development life cycle, and provides a template. The CIO stated that contingency plans should be developed in accordance to Special Publication 800-34 until DoD issues a formal contingency planning policy.

Audit Response. The CIO, Defense Threat Reduction Agency comments were partially responsive. While the CIO stated that contingency plans should be developed in accordance with Special Publication 800-34, he did not state whether the Defense Threat Reduction Agency would issue supplemental guidance requiring that system owners use Special Publication 800-34. We request that the Defense Threat Reduction Agency provide comments on the final report indicating whether the agency plans to issue supplemental guidance requiring that owners implement Special Publication 800-34 and the completion date for issuing the guidance.

Marine Corps Management Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Marine Corps is developing contingency plan templates based on Special Publication 800-34. The Director stated that, as part of the documents developed during DITSCAP, a system contingency plan is one of the required documents.

b. Require that the Designated Approving Authority, the Certifying Authority, the program manager, and the user representative approve contingency plans for information systems.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that current guidance requires that the contingency plan be included in the certification package. The Deputy for Information and Identity Assurance stated that the Designated Approving Authority reviews the certification package when determining the system's authority to operate.

Audit Response. ASD(NII)/CIO comments were partially responsive. While we agree that the Designated Approving Authority reviews the certification package when determining the system's authority to operate, the Deputy Assistant Secretary of Defense for Information and Identity Assurance did not comment on whether he would require the Designated Approving Authority, the Certifying Authority, the program manager, and the user representative to approve contingency plans for information systems. Therefore, we request that ASD(NII)/CIO provide comments on the final report clarifying the response to Recommendation 2.b.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army will comply with ASD(NII) contingency planning policy and procedures when promulgated. The Acting CIO stated that, as an interim measure, the Army will supplement Department of the Army Pamphlet 25-1-2 with best business practices on contingency planning procedures by November 30, 2007. The best business practices will have the Designated Approving Authority, the Certifying Authority, the program manager, and the user representative review, approve, and sign the contingency plan for any system in the acquisition process. The Certifying Authority, and the Designated Approving Authority will review and approve contingency plans for the installation network. The Acting CIO further stated that system owners are required by July 1, 2008, to review, update, and provide the Office of Information Assurance and Compliance a signed contingency plan for each system under their control.

Audit Response. The Army comments were responsive, and no further comments are required.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred in principle, stating that the Navy CIO will issue specific guidance on this subject after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments to the final report identifying a completion date for issuing supplemental guidance on the approval of contingency plans for Navy information systems.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that the approval authority for contingency plans that involve resources used by the Defense Information Systems Agency should reside with that agency. However, the Acting Director stated that a robust dialog must exist between the Defense Information Systems Agency and the Designated Approving Authority responsible for the system's certification and accreditation.

Audit Response. The Defense Contract Management Agency comments were partially responsive. A system whose contingency plan has been developed with resources from another agency should be jointly approved by the Defense Contract Management Agency and the Defense Information Systems Agency. We request that the Defense Contract Management Agency provide comments on the final report indicating how the agency will ensure that system contingency plans jointly funded with the Defense Information Systems Agency are approved.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that the agency's certification and accreditation process requires that the Designated Approving Authority, Certifying Authority, and program manager approve the System Security Authorization Agreement in accordance with DITSCAP. The CIO stated that the Defense Information System Agency plans to release an implementation manual in July 2008 that requires the four approving authorities to review the contingency plan before the System Security Authorization Agreement is approved.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency partially concurred, stating that current practice at the Defense Threat Reduction Agency requires that the Designated Approving Authority, Certifying Authority, program manager, and user representative approve system contingency plans. The CIO stated that, because it is difficult to find someone without a vested interest in system performance, the user representative functions defined in the DoD Information Assurance Certification Process should be optional.

Audit Response. The Defense Threat Reduction Agency comments were nonresponsive. Although the CIO stated that current practice at the Defense Threat Reduction Agency requires the Designated Approving Authority, Certifying Authority, program manager, and user representative to approve system contingency plans, those officials are not approving contingency plans as required. We request that the Defense Threat Reduction Agency provide comments on the final report indicating how the agency will ensure that its information system contingency plans are properly approved.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Designated Approving Authority is responsible for the final accreditation and acceptance of information assurance requirements for Marine Corps operational information systems. As part of the certification and accreditation process, the Certifying Authority or his representative review the system's documentation and provides an accreditation recommendation to the Designated Approving Authority for approval.

c. Require that system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum,

"Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006, and document results.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that DoD Instruction 8500.2 already requires that system owners test contingency plans. The Deputy for Information and Identity Assurance stated that amplifying guidance will be included in the FY 2008 FISMA reporting guidance on contingency plan testing.

Audit Response. ASD(NII)/CIO comments were responsive, and no further comments are required.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the existing guidance requires that system owners conduct recurring tests of contingency plans under a variety of conditions. The Acting CIO stated that the guidance also provides procedures for testing the security controls identified in DoD Instruction 8500.2.

Audit Response. The Army comments were partially responsive. While we recognize that the Army issued guidance requiring that owners conduct recurring tests of contingency plans under a variety of conditions, the Army CIO does not have controls in place to ensure that system owners comply with the policy. We request that the Army provide comments on the final report indicating how the Army will ensure that system owners are testing contingency plans under realistic conditions and in accordance with DoD Instruction 8500.2.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred, stating that the Navy CIO will issue specific guidance on this subject after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report indicating a completion date for issuing specific guidance on Recommendation 2.c.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency concurred, stating that tests of the contingency plan for the Agency's system were conducted annually. The Acting Director stated that an after-action report is published after each test.

Audit Response. The Defense Contract Management Agency comments were nonresponsive. The Defense Contract Management Agency system we reviewed did not develop or provide evidence of the system's contingency plan. The system owner could not conduct a test of a contingency plan that did not exist. The system owner did provide an after-action report for a test conducted of the continuity of operations plan for the Systems Management Center Ogden. However, we determined that the test was not of the system's contingency plan but a test of the Center's continuity of operations plan. Therefore, we request that the Defense Contract Management Agency provide comments on the final report

indicating whether the owner of the system we reviewed has since developed and then tested the system's contingency plan.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that an implementation manual scheduled for release in July 2008 will include procedures to enforce compliance with contingency plan requirements. The CIO stated that current procedures, taken from the annual DoD FISMA guidance, are provided to information assurance and program managers through a DoD online portal.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency nonconcurred, stating that resource constraints prevent recurring tests of contingency plans under realistic conditions. The CIO stated that desktop testing is economical and, if done properly, can be thorough enough to identify security weaknesses.

Audit Response. The CIO, Defense Threat Reduction Agency comments were nonresponsive. While we agree that desktop testing is economical and can identify security weaknesses, desktop testing does not provide the stringency to thoroughly identify security weaknesses of a contingency plan. For instance, testing backup and alternate site procedures to determine whether systems and the information they contain are available during a disruptive or catastrophic event would be best determined during a functional exercise. We request that Defense Threat Reduction Agency reconsider its position and allocate the resources needed to periodically conduct functional tests of its information system contingency plans.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Marine Corps implemented a quarterly reporting schedule requiring that Marine Corps information systems be tested in accordance with DoD Instruction 8500.2. The Director stated that the results are documented and used to update Marine Corps DITPR data as required by FISMA.

d. Implement management controls to verify that system owners:

(1) Develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

(2) Conduct recurring tests of system contingency plans in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security

Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006.

(3) Populate the "contingency plan" and "contingency plan last tested" data fields in the DoD Information Technology Portfolio Repository with complete and accurate system information.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, partially concurred with Recommendation 2.d.1., stating that DoD is using the interim DoD Information Assurance Certification and Accreditation Process, not DoD Instruction 5200.40. The Deputy for Information and Identity Assurance stated that additional guidance will be issued recommending that Special Publication 800-34 be used as a guide when preparing system contingency plans.

The Deputy for Information and Identity Assurance concurred with Recommendations 2.d.2. and 2.d.3., stating that plans are underway to conduct assessments to verify, among other things, that contingency plans are tested in accordance with current guidance and that Components maintain auditable documents that support information reported in DITPR.

Audit Response. ASD(NII)/CIO comments were partially responsive to Recommendation 2.d.1. and responsive to Recommendations 2.d.2. and 2.d.3. We request that ASD(NII)/CIO provide comments on the final report for Recommendation 2.d.1. that identify a completion date for issuing supplemental guidance requiring DoD Components to use Special Publication 800-34 when developing system contingency plans.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army Portfolio Management System is the official and authoritative source for information on Army information technology systems entered into DITPR. The Acting CIO stated that system owners enter their information into the Army Portfolio Management System, which is reviewed weekly by the Office of Information Assurance and Compliance to verify that system owners are developing contingency plans as required. The Acting CIO stated that owners with outdated plans are required to update the Army Portfolio Management System and provide a Plan of Action and Milestones indicating when they will become compliant. The Acting CIO stated that, currently, there are no independent methods to verify the accuracy of the data that owners enter into the Army Portfolio Management System.

The Acting CIO stated that the Army will begin requiring system owners to provide the Office of Information Assurance and Compliance with a copy of their authenticated contingency plans. The Acting CIO also stated that the Army plans to implement a best business practice by requiring that owners of mission-critical systems submit a digitally signed message to the Office of Information Assurance and Compliance certifying that they have completed annual testing of the system's contingency plan.

Audit Response. The Army comments were responsive, and no further comments are required.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred, stating that the Navy CIO is already implementing Recommendation 2.d.3.

Audit Response. The Navy comments were partially responsive. The Deputy CIO did not respond to Recommendations 2.d.1 or 2.d.2. We request that the Navy respond to the final report for Recommendations 2.d.1 and 2.d.2.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency concurred, stating that the DoD CIO instructed DoD personnel to disregard DoD Instruction 5200.40 and comply with draft DoD Instruction 8510.bb, the DoD Information Assurance Certification and Accreditation Process.

Audit Response. The Defense Contract Management Agency comments were nonresponsive. The Acting Director did not state what actions he would take to implement Recommendations 2.d.1 through 2.d.3. We request that the Defense Contract Management Agency provide comments on the final report specifying actions taken for Recommendations 2.d.1. through 2.d.3.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that, in February 2007, the agency began requiring directorates to submit monthly reports. The CIO stated that the directorates are notified monthly when a system is not compliant. The CIO also stated that the agency has developed an automated tool that provides oversight on the information.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency partially concurred, stating that contingency plans should be developed in accordance with the DoD Information Assurance Certification and Accreditation Process and tested annually.

Audit Response. The Defense Threat Reduction Agency comments were nonresponsive. The CIO did not state what actions he would take to implement Recommendations 2.d.1. through 2.d.3. Therefore, we request that the Defense Threat Reduction Agency provide additional comments on the final report specifying actions taken for Recommendations 2.d.1. through 2.d.3.

e. Impose sanctions on system owners who do not prepare and test their systems' contingency plans or enter complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO concurred in principle, stating that the DoD CIO will work with the DoD Components to identify ways to deal with system owners who do not prepare and test their

system's contingency plan or enter complete, accurate, and authoritative information in DITPR.

Audit Response. ASD(NII)/CIO comments were partially responsive. The Deputy Assistant Secretary of Defense for Information and Identity Assurance did not provide a completion date for imposing sanctions on system owners who do not prepare and test their system's contingency plans or enter complete, accurate, and authoritative information in DITPR. We request that ASD(NII)/CIO provide comments on the final report indicating a completion date for imposing sanctions needed for system owners that do not comply with Recommendation 2.e.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army CIO will impose appropriate sanctions on owners who do not comply with contingency planning policies and procedures. The Acting CIO stated that the sanction could include withholding funds, withdrawal of the authority to operate, or denial of network connectivity.

Audit Response. The Army comments were responsive, and no further comments are required.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred in principle, stating that the Navy CIO will issue specific guidance on this subject after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report indicating a completion date for issuing specific guidance on Recommendation 2.e.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that agency officials do not believe a mandatory requirement to impose sanctions is needed in all instances. The Acting Director stated that sanctions should not be imposed when an owner inadvertently enters incorrect data. The Acting Director stated that, in such instances, nondisciplinary action is appropriate.

Audit Response. The Defense Contract Management Agency comments were partially responsive. The Acting Director did not state what sanctions he would impose on system owners that routinely enter incorrect data in DITPR. Additionally, the Acting Director did not specify an alternate course of action for those system owners who inadvertently enter incorrect data into DITPR. We request that the Defense Contract Management Agency provide comments on the final report on planned sanctions for system owners who enter incorrect data into DITPR.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that the Senior Information Assurance Officer has the authority to issue a notice to deny a system's authority to operate that presents a threat to network security. The CIO stated that this process will be used to enforce compliance of system contingency plan testing.

Audit Response. The Defense Information Systems Agency comments were partially responsive. The CIO did not state what sanctions he planned to impose on system owners who entered incorrect information in DITPR. We request that the Defense Information Systems Agency provide comments on the final report specifying planned sanctions for system owners who enter incorrect data into DITPR.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency concurred in principle, stating that it is necessary to determine meaningful sanctions that will not compromise operational effectiveness or mission achievement.

Audit Response. The Defense Threat Reduction Agency comments were partially responsive. The CIO did not state what he planned to impose on system owners who entered incorrect information in DITPR. We request that the Defense Threat Reduction Agency provide comments on the final report specifying planned sanctions for system owners who enter incorrect data into DITPR.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the systems without complete security documentation, including contingency plans, will not receive accreditation. The Director stated that those systems will be reported to the Marine Corps CIO for further action.

f. Implement automated controls, if applicable, on the Component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that the DoD CIO continues to coordinate with the Components using automated systems to populate DITPR. The Deputy for Information and Identify Assurance stated that automated systems ensure that appropriate automated application controls are in place to ensure a high degree of DITPR data quality.

Audit Response. ASD(NII)/CIO comments were partially responsive. The Deputy Assistant Secretary of Defense for Information and Identity Assurance did not explain what coordination efforts are taking place with the Components to implement automated controls on the Component systems used to populate DITPR. We request that ASD(NII)/CIO provide comments on the final report on the coordination efforts underway to implement Recommendation 2.f.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army Portfolio Management Solution system, used to populate DITPR, is operated under strict configuration management. To implement the recommendation, the Acting CIO stated that Army officials are developing

engineering change proposals for the system's configuration control board. The Acting CIO stated that the proposed changes include making the "contingency plan" field mandatory, and requiring it to be populated with an appropriate response. The Acting CIO stated that blank responses will not be considered appropriate, and that cross checks will be performed to prevent duplicate reporting. The Acting CIO stated that the engineering change proposals will be submitted to the control board by January 10, 2008, with implementation planned by July 1, 2008.

Audit Response. The Army comments were responsive, and no further comments are required.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred, stating that the Navy CIO and the Office of the Secretary of Defense are studying the feasibility of automated controls. The Deputy CIO stated that, currently, the Navy CIO is conducting twice-monthly manual reviews.

Audit Response. The Navy comments were responsive, and no further comments are required.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that the agency does not use an automated system to populate DITPR. The Acting Director stated that an information assurance professional manually updates DITPR and the agency's Deputy CIO reviews those updates.

Audit Response. The Defense Contract Management Agency comments were partially responsive. While we acknowledge that the Defense Contract Management Agency does not use an automated system to populate DITPR, we need the agency to explain the controls it uses to ensure that system owners enter correct information into DITPR. Therefore, we request that the Defense Contract Management Agency provide comments on the final report on Recommendation 2.f.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that the agency is evaluating automated information assurance management tools for DoD-wide fielding. The CIO stated that, in the interim, the Office of the CIO is using an automated DITPR compliance tracking tool to ensure the data quality of FISMA-related fields.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency concurred in principle, stating that the agency does not use a system to populate DITPR. The CIO stated that the agency plans to implement automated controls using its certification and accreditation database to validate information downloaded from DITPR.

Audit Response. The Defense Threat Reduction Agency comments were partially responsive. We request that the Defense Threat Reduction Agency provide comments on the final report indicating a completion date for implementing automated controls. We also request that the Defense Threat Reduction Agency provide the standard operating procedure for the automated controls used for its certification and accreditation database.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Marine Corps has implemented a certification and accreditation support tool that interfaces with and reports to DITPR.

g. Prepare a Component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred, stating that when facts in the DoD OIG audit report support the presence of weaknesses, the Components should develop and track a Component-level Plan of Action and Milestones to ensure the completion of remedial actions.

Audit Response. ASD(NII)/CIO comments were partially responsive. A Plan of Action and Milestone is required for any system with identified weaknesses, including weaknesses identified in a DoD OIG report. System owners should develop a Plan of Action and Milestones immediately after a weakness is identified, regardless of how it was identified. We request that the Deputy Assistant Secretary of Defense for Information and Identity Assurance provide comments on the final report clarifying his response to Recommendation 2.g.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army will develop and issue an Army-level Plan of Action and Milestones within 90 days of the issuance of the DoD OIG final report.

Audit Response. Although the Army comments were responsive, we request that the Army provide comments on the final report identifying a completion date for the development of the Army-level Plan of Action and Milestones.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred in principle, stating that the Navy CIO will develop a Component-level Plan of Action and Milestones.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report indicating a completion date for Recommendation 2.g.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that the recommendation is not applicable because there are no existing security weaknesses related to contingency planning.

Audit Response. The Defense Contract Management Agency comments were nonresponsive. We reviewed one Defense Contract Management Agency information system, and it did not meet the development or testing requirements for a system contingency plan. We request that the Defense Contract Management Agency explain in comments on the final report the rationale for stating that there are no existing security weaknesses related to contingency planning when this audit report clearly indicates that there were.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that the Office of the CIO will prepare a Plan of Action and Milestones within 90 days of the issuance of the final report to ensure that mission critical systems comply with contingency planning requirements. The CIO also stated that the Office of the CIO will increase oversight of documentation in its functional processes.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency concurred in principle, stating that the agency submitted a Component-level Plan of Action and Milestones in conjunction with its FY 2007 FISMA report submission. The CIO stated that the plan addressed security weaknesses in contingency planning for its reported systems.

Audit Response. The Defense Threat Reduction Agency comments were partially responsive. Although we commend the Defense Threat Reduction Agency for developing a Component-level Plan of Action and Milestones, the agency should monitor the issues identified in the plan until they are resolved. Additionally, the agency should report the results in its FY 2008 response to the Federal Information Security Management Act.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Marine Corps fielded five two-person system security engineering teams to oversee operational information assurance implementation and validation. The Director stated that the teams' charter includes support to the information assurance officials for developing and reporting contingency after-action reporting and validating and remediating any security weaknesses found.

h. Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred,

stating that, when facts in the DoD OIG audit report support the presence of weaknesses, the Components should develop and track a Component-level Plan of Action and Milestones to ensure the completion of remedial actions.

Audit Response. ASD(NII)/CIO comments were partially responsive. A Plan of Action and Milestones is required for any system with identified weaknesses, including weaknesses identified in a DoD OIG report. System owners should develop a Plan of Action and Milestones immediately after a weakness is identified, regardless of how it was identified. We request that the Army provide comments on the final report clarifying its response to Recommendation 2.h.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the CIO will require system owners identified in this report to develop a Plan of Action and Milestones and submit it to the Office of Information Assurance and Compliance.

Audit Response. Although the Army comments were responsive, we request that the Army provide comments on the final report with a completion date for the development of the Army-level Plan of Action and Milestones.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred in principle, stating that the Navy CIO will issue specific guidance on this subject after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report indicating a completion date for Recommendation 2.h.

Defense Contract Management Agency Management Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that the recommendation does not apply to the Agency. The Acting Director stated that during a review, we identified a weakness with the Agency's system. The Acting Director stated that the system now has a compliant contingency plan in place that will be tested annually.

Audit Response. The Defense Contract Management Agency comments were partially responsive. We request that the Defense Contract Management Agency, in response to the final report, provide a copy of the compliant contingency plan for the system we reviewed.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that he will require system owners to submit a Plan of Action and Milestones within 90 days of the issuance of this final report to ensure that their systems are compliant with contingency planning requirements.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency concurred in principle, stating that the Agency initiated action to address security weaknesses with contingency planning using a system-level Plan of Action and Milestones.

Audit Response. The Defense Threat Reduction Agency comments were responsive, and no further comments are required.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Marine Corps will comply with the requirement in its annual FISMA message.

i. Review assertions made in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum, including whether the Component implemented automated controls, and certify the current state of security for the Components' information systems. Interview information assurance professionals to verify that the information in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum is accurate.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that the DoD CIO considers the information in the memorandums correct; however, an assessment of the facts stated in the memorandum will be conducted.

Audit Response. ASD(NII)/CIO comments were partially responsive. We request that ASD(NII)/CIO provide comments on the final report indicating a completion date for reviewing the assertions made in the Component's DITPR CIO memorandums.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Army is in the process of implementing and refining the automated controls used to validate entries in the Army Portfolio Management Solution system. Army officials stated that the Army Portfolio Management Solution system interfaces with DITPR.

Audit Response. The Acting CIO, Department of the Army comments were nonresponsive. The Acting CIO did not state whether he would review assertions made in the DITPR CIO Memorandum, including whether the Component implemented automated controls, and certify the current state of security for the Components' information systems. The Acting CIO also did not state whether he would interview information assurance professionals to verify that the information in the DITPR CIO Memorandum is accurate. Therefore, we request that the Army provide comments on the final report for Recommendation 2.i.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred, stating that the Navy CIO and the Office of the Secretary of Defense are studying the feasibility of automated controls.

The Deputy CIO stated that the Navy CIO will issue specific guidance on interviewing the information assurance professionals after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report indicating a completion date for Recommendation 2.i.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency concurred, stating that agency officials completed a review of its information in DITPR and verified that it is accurate.

Audit Response. The Defense Contract Management Agency comments were responsive, and no further comments are required.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that he is currently using an automated DITPR compliance-tracking tool to ensure the data quality of FISMA-related fields. The CIO stated that the agency plans to expand the tool to assist with tracking the compliance of non-FISMA DITPR fields.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency concurred in principle, stating that the recommendation is current practice at the agency.

Audit Response. The Defense Threat Reduction Agency comments were responsive, and no further comments are required.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that the Marine Corps has implemented an automated security documentation and tracking tool, which included contingency reporting as a functionality.

j. Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement.

ASD(NII)/CIO Comments. The Deputy Assistant Secretary of Defense for Information and Identity Assurance, responding for the DoD CIO, concurred in principle, stating that DoD Components should conduct the review and document results in accordance with current guidance. The Deputy for Information and Identity Assurance stated that the Components should report results in their FY 2008 FISMA report submissions.

Audit Response. ASD(NII)/CIO comments were responsive, and no further comments are required.

Army Comments. The Acting CIO, Department of the Army concurred, stating that the Office of Information Assurance and Compliance conducted a review and identified systems designated as mission critical and MAC III. The Acting CIO stated that the Office of Information Assurance and Compliance identified 14 systems with both designations and is contacting system owners and requiring that they justify in writing the mission criticality and MAC assignment. The Acting CIO stated that planned completion for this recommendation is January 10, 2008.

Audit Response. The Army comments were responsive, and no further comments are required.

Navy Comments. The Deputy CIO for Policy and Integration, responding for the Navy CIO, concurred in principle, stating that the Navy CIO will issue specific guidance on this subject after receipt of the final audit report.

Audit Response. The Navy comments were partially responsive. We request that the Navy provide comments on the final report indicating a completion date for Recommendation 2.j.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency partially concurred, stating that the recommendation does not apply to the Agency because it does not have any mission-critical systems designated as MAC III.

Audit Response. Although the Defense Contract Management Agency partially concurred, we consider comments responsive, and no further comments are required. While the CIO, Defense Contract Management Agency stated that the agency does not have any systems designated as mission critical and MAC III, systems designations are not static. We request that the agency be cognizant of such designations now, and in the future.

Defense Information Systems Agency Comments. The CIO, Defense Information Systems Agency stated that he will review all MAC III systems designated as mission critical within 90 days of the issuance of the final report. The CIO stated that the Agency will document the rationale for the designations and, if necessary, reclassify systems.

Audit Response. The Defense Information Systems Agency comments were responsive, and no further comments are required.

Defense Threat Reduction Agency Comments. The CIO, Defense Threat Reduction Agency partially concurred, stating that the rationale should be documented in the System Information Security Plan required by the DoD Information Assurance Certification and Accreditation Process.

Audit Response. The CIO, Defense Threat Reduction Agency comments were partially responsive. The rationale to designate a system as mission-critical

and MAC III should be documented somewhere in the system's certification and accreditation documentation. The CIO did not state, however, whether the agency would require that owners of its Agency's information systems document the rationale in certification and accreditation documentation. We request that the Defense Threat Reduction Agency provide comments to the final report on whether the agency plans to require that owners of its Agency's information systems document the rationale in certification and accreditation documentation.

Marine Corps Comments. Although not required to respond, the Director, Command, Control, Communications, and Computers concurred with the recommendation, stating that systems that the public does not have access to are designated as MAC III. The Director stated that the Marine Corps will work with owners and program managers to complete the review and documentation to validate mission-critical, mission-essential, and mission support status.

Management Comments Required

The U.S. Strategic Command and Business Transformation Agency did not comment on the draft report issued on October 2, 2007; therefore, we request that they provide comments on the final report. Although the Air Force and the U.S. Transportation Command commented on the draft report, the comments did not indicate concurrence with the recommendation, proposed actions, or completion dates. The Defense Logistics Agency, Missile Defense Agency, and TRICARE Management Activity concurred with the recommendations; however, those agencies did not indicate proposed actions or completion dates.

In response to the final report, we request that management provide additional comments on the recommendations. The comments should include elements in the following table.

Management Comments Required

Recommendation	Organization	Statement of Concurrence or Nonconcurrence	Statement of Proposed Action	Statement of Completion Date
2.a. through 2.j.	Air Force	needed	needed	needed
	U.S. Strategic Command	needed	needed	needed
	U.S. Transportation Command	needed	needed	needed
	Business Transformation Agency	needed	needed	needed

Management Comments Required

Recommendation	Organization	Statement of Concurrence or Nonconcurrence	Statement of Proposed Action	Statement of Completion Date
	Defense Logistics Agency	received	needed	needed
	Missile Defense Agency	received	needed	needed
	TRICARE Management Agency	received	needed	needed

Appendix A. Scope and Methodology

We conducted this performance audit from January 2007 through October 2007 in accordance with generally accepted government auditing standards. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Universe and Sample. We used the unclassified DITPR as our source of information to determine the universe of DoD mission-critical systems requiring information assurance certification and accreditation. We did not review systems reported in the classified DITPR. We queried DITPR to identify systems that met two criteria: each system had to require certification and accreditation, and be mission-critical. Systems requiring certification and accreditation criteria are required to have contingency plans that are tested on a regular basis. We reviewed only mission-critical systems because the loss of the system information would cause stoppage of warfighter operations or undermine mission support of warfighter operations.

We queried the unclassified DITPR on January 24, 2007, the date of our audit announcement. Our query resulted in a universe of 436 mission-critical systems requiring information assurance certification and accreditation. The 436 systems included 110 Army, 97 Navy, 85 Air Force, 50 Marine Corps, and 94 ODO. The DoD Inspector General (IG) Quantitative Methods Directorate developed a statistical sample plan for the 436 systems using a stratified sample design, which resulted in an audit sample of 240 systems. The audit sample consisted of 60 Army, 54 Navy, 50 Air Force, 26 Marine Corps and 50 ODO systems. See Appendix B for the 240 systems sampled.

We reviewed two contingency planning data fields in DITPR for the 240 information systems. The first was the "contingency plan" data field in which system owners report whether they developed a contingency plan for their system. We asked the Components that had reported having developed a contingency plan to provide the approved, signed copy of the contingency plan. The second data element was the data field in which system owners report the date they last tested their contingency plan. We requested that system owners provide after-action or lessons-learned reports or any other documentation to demonstrate that they tested the system's contingency plan on the date they reported in DITPR. We provided the Components with the information we extracted from DITPR on January 24, 2007.

We compared contingency plans, contingency plan testing documents, and CIO DITPR Certification Memorandums with the requirements identified in DoD Directive 5144.1, DoD Instruction 8500.2, DoD Instruction 5200.40, DoD Manual 8510.1-M, FYs 2006 FISMA Guidance, and FY 2006 DITPR Guidance. We interviewed information assurance officials from the Army, Navy, and Air Force CIO offices.

Statistical Sampling and Use of Technical Assistance. The Quantitative Methods Directorate developed the statistical sample design for the audit universe of 436 systems. We used two measures associated with the existence and testing of system contingency plans. The two measures required independent projections and were subject to Bonferroni corrections. We used a 95-percent individual confidence level to calculate the statistical projections, which resulted in an effective 90-percent overall confidence level due to Bonferroni adjustment. The projections apply to the universe of 436 information systems.

Tables A-1 and A-2 identify projections for the individual Components and overall for DoD. Our projections in Table A-1 show that we are 90 percent confident that the owners of between 244 and 283 DoD mission-critical information systems did not prepare a contingency plan for their system. The unbiased point estimate of 264 systems is the most likely number of systems with no contingency plan.

Table A-1. Systems Lacking Contingency Plans

Components	Lower Bound	Point Estimate	Upper Bound
Army	46	57	67
Navy	59	68	77
Air Force	61	68	75
Marine Corps	45	50	*
ODO	12	21	29
Total DoD**	244	264	283

* Due to all sample systems with problems, projections are calculated using Exact Binomial distribution with one-tail and an effectively reduced confidence level for multiple estimates.

** Total DoD projections are computed independently and do not reflect the totals of the three columns.

Our projections in Table A-2 show that we are 90 percent confident that owners of between 342 and 373 mission-critical information systems did not test or could not provide evidence of testing their systems' contingency plans. The unbiased point estimate of 358 systems is the most likely number of systems untested contingency plans.

Table A-2. Contingency Plans Lacking Testing

Component	Lower Bound	Point Estimate	Upper Bound
Army	90	97	104
Navy	80	86	93
Air Force	79	85	*
Marine Corps	45	50	*
ODO	30	39	49
Total DoD**	342	358	373

* Due to all sample systems with problems, projections are calculated using Exact Binomial distribution with one-tail and an effectively reduced confidence level for multiple estimates.

** Total DoD projections are computed independently and do not reflect the totals of the three columns.

Our projections in Table A-3 show that we are 90 percent confident of the following.

- Owners of between 23 and 50 DoD mission-critical information systems did not correctly report in DITPR whether they had developed contingency plans for their systems. The unbiased point estimate of 37 systems is the most likely number of systems with incorrect information in the "contingency plan" data field in DITPR.

- Owners of between 398 and 422 DoD mission-critical information systems did not correctly report in DITPR whether they had tested their systems' contingency plans. The unbiased point estimate of 410 systems is the most likely number of systems with incorrect information in the "contingency plan last tested" data field in DITPR.

Table A-3. Systems With Inaccurate Information in DITPR

Component	Lower Bound	Point Estimate	Upper Bound
Reporting of Contingency Plan Not Accurate	23	37	50
Reporting of Contingency Plan Testing Not Accurate	398	410	422

Use of Computer-Processed Data. We did not use computer-processed data to perform this audit. We used the DITPR database for determining the audit universe and sample. DITPR, however, does not process data. The DoD Components populate DITPR through data entry.

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 areas.

Prior Coverage

During the last 5 years, DoD IG issued four reports discussing DITPR. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

DoD IG

DoD IG Report No. D-2007-099, "DoD Privacy Program and Privacy Impact Assessments," June 13, 2007

DoD IG Report No. D-2006-042, "Security Status for Systems reported in DoD Information Technology Databases," December 30, 2005

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

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

Appendix B. DoD Mission-Critical Systems Sampled

We reviewed contingency planning information for the following 240 mission-critical systems as of January 24, 2007. We listed the systems first by Component, then by DITPR identification number. System owners continue to leave DITPR data fields blank or select "n/a" when reporting system information. Based on audit analysis, the "Contingency Plan Met Requirements" column indicates whether the system contingency plan met requirements listed in Appendix A.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
	Army				
1		81	yes	no	Nov. 6, 2006*
2		85	yes	no	May 4, 2006*
3		86	yes	yes	March 30, 2006
4		566	yes	yes	May 6, 2006*
5		568	yes	no	May 16, 2006*
6		605	yes	yes	May 6, 2006*
7		1205	yes	no	Jan. 8, 2006*
8		1207	yes	yes	Jan. 8, 2006*
9		1217	yes	yes	Jan. 8, 2006*
10		1292	yes	no	March 30, 2006*
11		2540	yes	yes	June 6, 2006*
12		2561	yes	yes	Sept. 15, 2006*
13		2638	yes	yes	May 5, 2006*
14		2641	yes	no	March 14, 2006*
15		2652	yes	no	June 16, 2006*
16		2660	no	no	May 19, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
17		2668	yes	yes	May 6, 2006*
18		2672	yes	yes	May 31, 2006*
19		2675	yes	no	June 14, 2006*
20		2707	no	yes	March 22, 2006*
21		2727	yes	no	Feb. 28, 2006*
22		2894	yes	no	Aug. 8, 2006*
23		2933	yes	yes	April 24, 2006*
24		2960	yes	yes	Feb. 15, 2006*
25		2984	yes	no	June 26, 2006*
26		2992	yes	yes	May 12, 2006*
27		2993	yes	yes	May 12, 2006*
28		3032	yes	yes	April 20, 2006*
29		3037	blank	yes	July 19, 2006*
30		3052	no	yes	Jan. 10, 2006*
31		3325	blank	yes	April 27, 2006*
32		3340	yes	no	April 12, 2006*
33		3378	yes	no	Jan. 30, 2006*
34		3379	no	yes	Oct. 27, 2006*
35		3381	yes	yes	March 30, 2006
36		3459	yes	no	June 30, 2006*
37		3565	yes	no	Feb. 28, 2006*
38		3612	yes	no	May 4, 2006*
39		3668	blank	no	blank*
40		3674	yes	yes	July 14, 2006*
41		3712	yes	no	May 1, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
42		3714	blank	no	blank*
43		3719	blank	yes	Sept. 18, 2006*
44		3808	yes	no	May 1, 2006*
45		3813	yes	yes	Aug. 25, 2006*
46		3872	yes	yes	Oct. 19, 2006*
47		3896	yes	no	March 29, 2006*
48		3897	yes	no	Feb. 27, 2006*
49		3905	yes	yes	Aug. 16, 2006*
50		3918	yes	no	Aug. 15, 2006*
51		3983	yes	yes	Aug. 25, 2006*
52		3990	no	no	Oct. 10, 2006*
53		4019	yes	yes	Dec. 1, 2006*
54		4034	yes	no	July 31, 2006*
55		4078	yes	no	March 14, 2006*
56		4079	yes	no	March 14, 2006*
57		4096	yes	no	March 14, 2006*
58		5188	yes	no	July 31, 2006*
59		5910	yes	yes	March 12, 2006*
60		8470	yes	no	May 15, 2006*
	Navy				
61		118	yes	yes	May 15, 2006*
62		320	yes	no	May 18, 2006*
63		4370	yes	no	June 29, 2006*
64		4393	yes	yes	Aug. 11, 2006*
65		4397	yes	yes	Jan. 23, 2006

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
66		4430	yes	no	Aug. 26, 2006*
67		4432	yes	no	Aug. 22, 2006*
68		4433	yes	yes	June 2, 2006*
69		4449	yes	no	Aug. 23, 2006*
70		4514	yes	no	March 14, 2006*
71		4516	yes	no	Aug. 24, 2006*
72		4528	yes	yes	May 5, 2006*
73		4559	yes	yes	Oct. 10, 2006*
74		4567	yes	no	Aug. 1, 2006*
75		4652	no	no	Jan. 17, 2007*
76		4654	no	no	Jan. 17, 2007*
77		4736	yes	no	March 16, 2006*
78		4764	yes	no	Feb. 28, 2007*
79		4766	yes	no	Jan. 17, 2007*
80		4800	yes	no	July 19, 2006*
81		4807	yes	no	Aug. 23, 2006*
82		4812	yes	yes	March 24, 2006*
83		4813	yes	yes	May 19, 2006*
84		4821	yes	yes	March 27, 2006*
85		4827	yes	yes	May 18, 2006*
86		4830	yes	yes	Oct. 24, 2002*
87		4836	yes	no	Dec. 5, 2006*
88		4871	yes	no	Aug. 22, 2006*
89		4927	yes	no	June 29, 2006*
90		4932	n/a	no	June 27, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
91		4934	yes	no	Dec. 18, 2006*
92		4947	yes	yes	July 31, 2006
93		4953	yes	no	March 27, 2006*
94		4986	yes	no	Nov. 1, 2005*
95		4989	no	no	Jan. 17, 2007*
96		5002	yes	no	Sept. 15, 2005*
97		5011	yes	yes	Feb. 13, 2006*
98		5016	yes	no	July 31, 2006*
99		5021	yes	no	Feb. 23, 2006*
100		5035	yes	no	March 5, 2006*
101		5038	yes	no	Aug. 22, 2006*
102		5042	yes	yes	May 10, 2006*
103		5050	yes	no	April 15, 2006*
104		5117	yes	no	May 25, 2006*
105		5119	yes	no	Oct. 22, 2006*
106		5125	yes	no	April 15, 2006*
107		5166	yes	yes	Oct. 8, 2007*
108		6872	yes	no	July 1, 2006*
109		6971	yes	no	Sept. 15, 2006*
110		6978	yes	no	July 23, 2006*
111		8069	yes	no	Feb. 28, 2006*
112		8163	yes	yes	Aug. 24, 2006*
113		8577	blank	no	Sept. 14, 2006*
114		8849	blank	no	Jan. 27, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
	Marine Corps				
115		4416	yes	no	July 27, 2006*
116		4418	yes	no	July 27, 2006*
117		4420	yes	no	July 27, 2006*
118		4424	yes	no	July 27, 2006*
119		4440	yes	no	July 27, 2006*
120		4517	yes	no	July 27, 2006*
121		4538	yes	no	July 27, 2006*
122		4718	yes	no	July 27, 2006*
123		4720	yes	no	July 27, 2006*
124		4732	yes	no	July 27, 2006*
125		4740	yes	no	July 27, 2006*
126		4784	yes	no	July 27, 2006*
127		4798	yes	no	July 27, 2006*
128		4864	yes	no	July 27, 2006*
129		4941	yes	no	July 27, 2006*
130		4970	yes	no	July 27, 2006*
131		4992	yes	no	July 27, 2006*
132		5020	yes	no	July 1, 2006*
133		5028	yes	no	July 27, 2006*
134		5061	yes	no	July 27, 2006*
135		5081	yes	no	July 27, 2006*
136		5095	yes	no	July 27, 2006*
137		5096	yes	no	July 27, 2006*
138		5100	yes	no	July 27, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
139		5108	yes	no	July 27, 2006*
140		5143	yes	no	July 27, 2006*
	Air Force				
141		451	yes	yes	June 13, 2006*
142		879	yes	yes	Aug. 27, 2006*
143		939	yes	no	June 3, 2006*
144		942	yes	no	June 15, 2006*
145		1049	yes	yes	Aug. 23, 2006*
146		1298	yes	yes	Jan. 30, 2006*
147		1460	yes	no	June 30, 2006*
148		1711	yes	no	July 14, 2006*
149		1725	yes	no	Aug. 6, 2006*
150		1848	yes	yes	April 1, 2005*
151		1876	yes	no	March 7, 2006*
152		1948	yes	no	July 15, 2002*
153		2004	yes	no	May 12, 2006*
154		2049	yes	no	June 1, 2004*
155		2077	yes	no	Aug. 11, 2006*
156		2143	yes	no	blank*
157		2145	yes	no	blank*
158		2173	yes	no	Jan. 18, 2006*
159		2223	yes	no	Aug. 3, 2006*
160		2226	yes	no	March 3, 2005*
161		2229	yes	yes	Nov. 20, 2006*
162		2395	yes	no	Oct. 25, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
163		2448	yes	no	July 1, 2006*
164		2454	yes	no	Oct. 30, 2006*
165		5851	yes	no	Oct. 20, 2006*
166		5885	yes	no	Aug. 15, 2004*
167		6666	yes	no	June 15, 2006*
168		7164	yes	no	July 14, 2006*
169		7319	yes	no	April 26, 2006*
170		7728	yes	no	Oct. 28, 2005*
171		7743	yes	no	June 21, 2006*
172		7778	yes	no	Oct. 18, 2006*
173		7796	yes	yes	March 31, 2006*
174		7797	yes	no	Jan. 12, 2006*
175		7798	yes	no	Nov. 16, 2005*
176		7799	yes	no	Nov. 22, 2005*
177		7801	yes	yes	Jan. 12, 2006*
178		7802	yes	no	Jan. 19, 2006*
179		7803	yes	no	Jan. 23, 2006*
180		7804	yes	no	Jan. 23, 2006*
181		7806	yes	no	Jan. 12, 2006*
182		7820	yes	no	Feb. 10, 2006*
183		7854	yes	no	Nov. 11, 2006*
184		7864	yes	no	Dec. 19, 2005*
185		8265	yes	no	July 18, 2006*
186		8321	yes	yes	July 14, 2006*
187		8351	yes	no	Jan. 12, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
188		8367	yes	no	Jan. 23, 2006*
189		8751	yes	no	Aug. 16, 2006*
190		8752	yes	yes	April 14, 2006*
	U.S. Transportation Command				
191		348	yes	yes	Jan. 10, 2007
192		349	yes	no	March 2, 2006*
193		354	yes	yes	May 18, 2006*
194		359	yes	yes	Nov. 1, 2006
195		369	yes	yes	Nov. 7, 2006*
196		370	yes	yes	Jan. 15, 2006*
197		374	yes	yes	June 15, 2006
198		376	yes	yes	July 7, 2006
199		487	yes	yes	July 7, 2006
200		1352	yes	yes	July 19, 2006*
201		3093	yes	yes	Feb. 6, 2006*
202		3112	yes	yes	April 10, 2006
203		4227	yes	yes	June 19, 2006*
204		4238	yes	yes	Oct. 23, 2006*
	U.S. Strategic Command				
205		3120	yes	yes	Dec. 8, 2006*
	ASD(NII)/CIO				
206		3264	yes	yes	Sept. 28, 2005*
	Business Transportation Agency				
207		6501	blank	yes	Oct. 23, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
	Defense Contract Management Agency				
208		423	yes	no	Feb. 3, 2006*
	Defense Information Systems Agency				
209		3106	yes	no	May 27, 2005*
210		3150	yes	yes	May 17, 2006*
211		3189	yes	no	April 8, 2006*
212		3194	yes	yes	May 25, 2006*
213		3196	yes	yes	Nov. 12, 2006*
214		3200	yes	yes	May 21, 2006*
215		3205	yes	no	Aug. 6, 2006
216		3210	yes	yes	March 3, 2006*
217		3212	yes	yes	June 14, 2006*
218		3220	yes	yes	May 19, 2006*
219		3224	yes	yes	Aug. 1, 2005*
220		3236	yes	no	April 18, 2006*
221		3245	yes	yes	July 10, 2006*
222		3249	yes	yes	Sept. 26, 2006*
223		3253	yes	no	April 18, 2006*
224		3259	yes	yes	June 17, 2006*
225		7496	yes	yes	May 19, 2006*
226		7895	yes	yes	July 10, 2006*
227		7902	blank	no	Aug. 6, 2006
228		7903	yes	yes	March 11, 2006*
229		8546	blank	no	July 2, 2005*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Sampled System	Component	DITPR Identification Number	Component Reported Contingency Plan Developed	Contingency Plan Met Requirements	Component Reported Date Contingency Plan Last Tested
	Defense Logistics Agency				
230		280	yes	yes	July 28, 2003*
231		281	yes	yes	Feb. 28, 2004*
232		286	yes	yes	Dec. 2, 2005
233		288	yes	yes	Aug. 17, 2006
234		8563	yes	yes	Aug. 16, 2006*
	Defense Threat Reduction Agency				
235		3183	yes	yes	Oct. 21, 2005*
236		4260	yes	yes	Oct. 21, 2005*
237		7550	no	no	blank*
	Missile Defense Agency				
238		4295	yes	no	Aug. 23, 2006*
	TRICARE Management Agency				
239		138	yes	yes	April 13, 2006*
240		164	yes	yes	Oct. 31, 2006*

* Based on the analysis of the evidence system owner provided, the owner did not report the correct date in DITPR of the last test of the system's contingency plan.

Appendix C. Management Comments on the Finding, Unsolicited Comments on the Finding and Recommendations, and Audit Response

The Air Force, U.S. Transportation Command, and the Defense Contract Management Agency provided comments on the finding section of the report. Although not required to comment, the Marine Corps also commented on the finding and the Defense Threat Reduction Agency commented on Recommendation 1.

Management Comments on the Finding, and Audit Response

Air Force Comments. The CIO, Air Force stated that on April 17, 2007, he released a detailed Instruction on contingency plan development, which was included in the Air Force FY 2007 FISMA Reporting Guidance. The Air Force CIO stated that the Air Force FY 2007 FISMA Reporting Guidance required system owners to use Special Publication 800-34 to develop and maintain a viable contingency planning program. The Air Force CIO stated that the Air Force plans to incorporate contingency planning procedures in Special Publication 800-34 into Air Force policy. The CIO also stated that the Air Force will audit contingency plan development and testing plan to ensure gaps are identified, training is relevant, and exercises are conducted and documented to improve plan effectiveness.

Audit Response. We commend the Air Force for taking corrective action on some of the issues identified in this report.

U.S. Transportation Command Comments. The Director, Program Analysis and Financial Management, commenting for the U.S. Transportation Command CIO, stated that the one system contingency plan we determined did not meet requirements was updated and subsequently tested in July 2007. The Director also stated that six of the eight systems we determined did not have correct contingency plan test dates in DITPR were tested in accordance with DoD policy; however, the DITPR Guidance allows owners 30 days to update their system information in DITPR. The Director stated that he attributed the incorrect dates in DITPR to the latency requirement for reporting information in DITPR.

The Director further said that the U.S. Transportation Command developed and standardized templates, based on DoD Instruction 8500.2, to assist system managers in developing contingency plans and documenting plan results. The Director stated that U.S. Transportation Command requested and receives Plans of Actions and Milestones from system managers, continuously monitors the plans, and assists managers when they submit inadequate documentation.

Audit Response. We commend the U.S. Transportation Command for taking corrective action on some of the issues identified in this report.

Defense Contract Management Agency Comments. The Acting Director, Defense Contract Management Agency stated that owners of Defense Contract Management Agency systems have contingency plans. The Acting Director stated that the Defense Information Systems Agency hosts and operates the system we reviewed and prepared a contingency plan for the system. The Acting Director stated that although the owner of the system reported an incorrect date in DITPR in January 2007, the agency entered the correct date on May 15, 2007, and promptly notified our office.

Audit Response. We commend the Defense Contract Management Agency for taking corrective action on some of the issues identified in this report.

Unsolicited Comments on the Finding, and Audit Response

Marine Corps Comments. The Director, Marine Corps Command, Control, Communications and Computers stated that, to meet information assurance reporting requirements, the Marine Corps identified three enclaves. The enclaves include garrison and tactical information systems and networks located in or on Marine Corps bases, posts, camps, stations, and major subordinate commands. The Director stated that all networks, networked systems, and other information systems are certified and accredited to operate in one of the three enclaves and documented in the approved enclave System Security Authorization Agreement.

The Director stated that the Marine Corps agreed with the findings that system owners for 100 percent of Marine Corps information systems did not show that contingency plans were developed and tested. The Director stated that the Marine Corps will demonstrate system accountability in a Plan of Action and Milestones. The Director further stated that although the initial submission of test and after action reports did not explicitly identify the systems under review, additional documents were provided indicating the location of each system and to which enclave the system belonged.

Audit Response. Marine Corps system owners provided one document during their initial submission of documents for all 26 systems sampled—an appendix from the Marine Corps Logistics Command Security System Authorization Agreement—as evidence that they had prepared contingency plans for the 26 systems. Marine Corps system owners also provided a memorandum stating that the appendix covered contingency planning procedures for the 26 systems under review. The five-page appendix, however, did not mention the 26 systems or provide contingency planning procedures for the systems.

Prior to a briefing we conducted with Marine Corps officials on the preliminary results of this audit, Marine Corps officials provided a spreadsheet that identified the locations of the 26 Marine Corps information systems we reviewed. The spreadsheet, however, did not identify the enclave to which the 26 systems belonged. Additionally, the spreadsheet indicated that only 4 of the 26 systems we reviewed were covered by the Marine Corps Logistics Command Security System Authorization Agreement, the only document they provided us initially. We did not consider the spreadsheet sufficient evidence that owners of the 26 systems we reviewed developed and tested the systems' contingency plans. The system

boundaries and enclaves to which the system belongs should be recorded in the system's certification and accreditation documents, not in a spreadsheet generated specifically for the audit team.

Unsolicited Comments on the Recommendations

Defense Threat Reduction Agency Comments. Although not required to respond, the CIO, Defense Threat Reduction Agency commented on Recommendation 1. The CIO stated that the lack of detailed DoD guidance on contingency planning impedes the Agency's ability to develop, test, and approve contingency plans for information systems. The CIO stated that the Agency would benefit from a supplement on testing contingency plans and improving its DITPR data quality and integrity. The CIO also stated that clarification of the definitions for contingency plan and continuity of operation plans would eliminate inappropriate substitution of one term for the other. Lastly, the CIO stated that implementation of a training program in contingency planning would benefit the Agency by developing individuals with the skills to complete contingency plans.

Appendix D. 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 Health Affairs/Chief Information Officer
Assistant Secretary of Defense for Networks and Information Integration/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

Auditor General, Department of the Army
Chief Information Officer, Department of the Army

Department of the Navy

Auditor General, Department of the Navy
Chief Information Officer, Department of Navy
Deputy Chief Information Officer, U.S. Marine Corps
Naval Inspector General
Assistant Secretary of the Navy (Manpower and Reserve Affairs)

Department of the Air Force

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

Combatant Commands

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

Other Defense Organizations

Director, Defense Contract Management Agency
Director, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, Defense Threat Reduction Agency
Director, Missile Defense Agency
Director, TRICARE Management Activity
Chief Information Officer, U.S. Mission North Atlantic Treaty Organization
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 Information Systems Agency
Chief Information Officer, Defense Logistics Agency
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 Threat Reduction Agency
Chief Information Officer, Missile Defense Agency
Chief Information Officer, Pentagon Force Protection Agency
Chief Information Officer, Armed Forces Information Service
Chief Information Officer, Defense Technical Information Center
Chief Information Officer, Defense Technology Security Administration
Chief Information Officer, Department of Defense Education Activity
Chief Information Officer, Defense Human Resource Activity
Chief Information Officer, DoD Test Resources Management Center
Chief Information Officer, TRICARE Management Activity
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 Homeland Security and Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Oversight and Government Reform
House Subcommittee on Government Management, Organization, and Procurement, Committee on Oversight and Government Reform
House Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform
House Subcommittee on Technology and Innovation, Committee on Science and Technology

Assistant Secretary of Defense for Networks and Information Integration Comments

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

NETWORKS AND INFORMATION INTEGRATION

NOV 09 2007

MEMORANDUM FOR INSPECTOR GENERAL, DEPARTMENT OF DEFENSE

SUBJECT: Draft Report on Contingency Planning for DoD Mission-Critical Information Systems (Project No. D2007-D000LB-0080.000)

The DASD(IIA) appreciates the opportunity to comment on the subject draft report.

In general, this office agrees that the report raises concerns about the current state of contingency planning for mission-critical systems within of the Department which must be addressed. Specific comments on the sixteen recommendations in the draft report are provided in the attachment.

My Primary Action Officer is: Mr. John Hunter, 703 602-9927, (DSN) 332-9927, john.hunter@osd.mil or john.hunter@osd.smil.mil.

Robert F. Lentz
Deputy Assistant Secretary of Defense
Information and Identity Assurance

Attachments:
As stated

DoDIG Report Dated October 2, 2007
PROJECT NO. D2007-D000LB-0080.000

"Contingency Planning for DoD Mission-Critical Information Systems"

DEPARTMENT OF DEFENSE COMMENTS
TO THE OIG RECOMMENDATIONS

RECOMMENDATION 1a: The OIG recommends that the ASD(NII)/DoD CIO, require DoD Components to use the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, when developing and testing DoD contingency plans, or issue a comprehensive DoD contingency planning policy. (p.15)

DoD CIO RESPONSE: Concur in principle. The DoD CIO will recommend that the NIST Special Publication be used as a guide for preparing contingency plans. Some of the specific techniques specified in the special publications do not conform to DoD business practices and must be adapted for use by the components, thereby precluding the DoD CIO from "requiring" its use.

RECOMMENDATION 1b: Inform the Office of Management and Budget and Congress that DoD does not have internal controls over the accuracy of data on the security of its information technology systems, and include a caveat to that effect in all reports based on data drawn from the DoD Information Technology Portfolio Repository until demonstrably effective internal controls have been in place for at least 1 full year. (p.15)

DoD CIO RESPONSE: Concur in principle. The subject audit only addressed Contingency Planning data elements in DITPR so broad assertions on the overall quality of data in DITPR are not supported by the small number of data elements sampled as part of this audit. However, future reports generated using the DITPR as the principal source will include a caveat indicating that some DITPR data should be used with caution, if appropriate.

RECOMMENDATION 1c: Immediately issue a supplement to the DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) for Fiscal Year 2007 (FY07)," May 21, 2007, and all continuations of the guidance, that contains information on testing contingency plans that was included in the supplemental section of the DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006. (p.15)

DoD CIO RESPONSE: Partially-concur. Since the FY2007 reporting is complete a supplement to that guidance would serve no useful purpose. Additional guidance on contingency planning and testing will be included in the FY2008 guidance which will be issued in the first calendar quarter of 2008.

RECOMMENDATION 1d: Immediately issue a supplement to the DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008," September 6, 2007, and all continuations of the guidance that:

> **(1) Defines an automated control and specifies the types of data integrity rules DoD Components must implement to ensure they supply complete, accurate, and authoritative data in the DoD Information Technology Portfolio Repository.**
> **(2) Clarifies the difference between a contingency plan and a continuity of operations plan.**
> **(3) Removes reference to continuity of operations plans in the "contingency plan" and "contingency plan last exercised" data fields in the DoD Information Technology Portfolio Repository and the DoD Information Technology Portfolio Repository Data Dictionary.**
> **(pp.15/16)**

DoD CIO RESPONSE: Concur in principle. The DoD CIO position is that many new features to enhance the quality of DITPR data were introduced in the October 2007 Block 4 release of the software, and that additional changes to institute automated application controls have been determined and will be introduced into subsequent releases. Steps will also be taken to supplement the guidance to clarify the differences between contingency planning and continuity of operations planning.

RECOMMENDATION 1e: Implement a training program in contingency planning for DoD Component officials who develop, test, and approve contingency plans for information systems. (p.16)

DoD CIO RESPONSE: Concur. The DoD will add additional guidance on contingency planning to the IT information assurance training program managed and operated for the Department by the Defense Information Systems Agency.

RECOMMENDATION 2: The OIG recommends that the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer; the Director, Business Transformation Agency; and the Chief Information Officers for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the Defense Contract Management Agency, the Defense Threat Reduction Agency, the Defense Information Systems Agency, the Defense Logistics Agency, the Missile Defense Agency and the TRICARE Management Activity:

a. Require that system owners develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy. (p. 20/GAO Report)

DoD CIO RESPONSE: Non-concur. The Department is currently operating under Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation (C&A) Process (DIACAP) Guidance dated July 6, 2006 in place of DoD Instruction 5200.40. As stated above additional guidance will be provided recommending that NIST Special Publication be used as a guide when preparing contingency plans. Some of the specific techniques specified in the special publications do not conform to DoD business practices and must be adapted for use by the components, thereby precluding the DoD CIO from "requiring" its use. Additional guidance concerning contingency plans will also be included in the DoD Information Security Certification and Accreditation Program Knowledge Service.

RECOMMENDATION 2b: Require that the Designated Approving Authority, the user representative, the program manager, and the Certifying Authority approve contingency plans for information systems. (p.16)

DoD CIO RESPONSE: Concur in principle. All of the above are involved either in developing, evaluating or approving contingency plans as a part of the overall DoD information system acquisition process. Current guidance requires that the contingency plan be a part of the certification package which must be considered by the DAA when determining the authorization to operate

RECOMMENDATION 2c: Require that system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006, and document results. (p.16)

DoD CIO RESPONSE: Concur in principle. DoD Instruction 8500.2 already requires that the system owners test contingency plans. Amplifying guidance will be included in the FY2008 FISMA Reporting guidance on contingency plan testing.

RECOMMENDATION 2d (1): Implement management controls to verify that system owners:

(1) Develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997 and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. (p.16)

DoD CIO RESPONSE: Partially-concur. The Department is currently operating under the Interim DIACAP, dated July 6, 2006 in place of DoD Instruction 5200.40. As stated above, additional guidance will be provided recommending that NIST Special Publication 800-34 be used as a guide when preparing contingency plans. Some of the specific techniques specified in the special publications do not conform to DoD business practices and must be adapted for use by the components, thereby precluding the DoD CIO from "requiring" its use. Plans are underway to conduct DoD CIO FISMA Compliance assessments to verify among other things that contingency plans are developed in accordance with component guidance.

RECOMMENDATION 2d (2): Implement management controls to verify that system owners:

Conduct recurring tests of system contingency plans in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006. (p.16)

DoD CIO RESPONSE: Concur. Plans are underway to conduct DoD CIO FISMA Compliance assessments to verify among other things that contingency plans are tested in accordance with current guidance.

RECOMMENDATION 2d (3): Implement management controls to verify that system owners:

Populate the "contingency plan" and "contingency plan last tested" data fields in the DoD Information Technology Portfolio Repository with complete and accurate system information. (p.17)

DoD CIO RESPONSE: Concur. Plans are underway to conduct DoD CIO FISMA Compliance assessments to verify among other things that components maintain auditable documentation that supports the information reported in DITPR.

RECOMMENDATION 2e: Impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository. (p.17)

DoD CIO RESPONSE: Concur in principle. The DoD CIO will work with the DoD Components to devise ways and means to appropriately deal with system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository.

RECOMMENDATION 2f: Implement automated controls, if applicable, on the Component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields. (p.17)

DoD CIO RESPONSE: Concur in principle. The DoD CIO will continue to coordinate closely with the components which use automated feeder systems to populate the DITPR to ensure the appropriate automated application controls are in place to assure a high degree of quality in DITPR data.

RECOMMENDATION 2g: Prepare a Component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning. (p.17)

DoD CIO RESPONSE: Concur. The DoD CIO position is that it is appropriate for the Components to verify the information in the OIG audit report and where the facts support the presence of weaknesses that a Component-level POA&M be developed and tracked to ensure remedial actions are completed.

RECOMMENDATION 2h: Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report. (p.17)

DoD CIO RESPONSE: Concur. The DoD CIO position is that it is appropriate for the Components to verify the information in the OIG audit report and where the facts support the presence of weaknesses that systems owners develop a POA&M and track progress to ensure remedial actions are completed.

RECOMMENDATION 2i: Review assertions made in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems. Interview the information assurance professionals to verify that the information in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum is accurate. (p.17)

DoD CIO RESPONSE: Concur. The DoD CIO position is that information provided is correct, however, an assessment of the facts stated in the memorandum will be undertaken.

RECOMMENDATION 2j: Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement. (p.17)

DoD CIO RESPONSE: Concur in principle. The review should be undertaken by the DoD Components, with the results documented in accordance with current guidance, and reported as part of their submission to the FY2008 annual FISMA report.

Department of the Army Comments

DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office, Chief Information Officer / G-6

NOV 15 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL, 400 ARMY NAVY DRIVE, ARLINGTON, VA 22202-4704

SUBJECT: Army Management Comments to Draft Report on Contingency Planning for DoD Mission Critical Information Systems, Project No. D2007-D000LB-0080.000

Reference the draft audit report Contingency Planning for DoD Mission-Critical Information Systems, Project No. D2007-D000LB-0080.000 addressing the reliability of contingency planning data reported in the Department of Defense Information Technology Portfolio Repository (DITPR). The report identified that DoD Component Chief Information Officer's (CIO's) did not implement management controls to verify that system owners developed and tested system contingency plans as required, and that the Component CIO's did not implement Component level automated controls to ensure complete and accurate reporting in the DITPR.

We are in general agreement with your findings and will work with the Office of the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer to develop policies and procedures to ensure adequate controls are in place.

In the enclosed management comment document we respond to each of the recommendations made to the Department of the Army CIO, identify those corrective actions that have been or are being implemented, and, where appropriate, provide the estimated date of completion of each action.

We appreciate the insight your audit has provided. My point of contact for this audit is Mr. Gary A. Robison, telephone 703 602-7395, e-mail: gary.robison@us.army.mil .

Randolph P. Strong
for Vernon M. Bettencourt, Jr.
Acting Chief Information Officer/G-6

Encl

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 1. Recommendations 1a through 1e are addressed to the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer.

Army Comment: Army makes no comment to recommendations 1a through 1e.

Recommendation 2 a.

"We recommend that the ...Chief Information Officer for the Department of the Army...Require that system owners develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy."

Army Comment:

Concur. Department of the Army has published DA PAM 25-1-2, Information Technology Contingency Planning, dated 16 November 2006. Its emphasis is on identifying and describing implementing procedures, explicit and implied, stemming from Defense policies and Federal authorities, to include Title 40, United States Code, Chapter 25, Subchapter III) (40 USC 1401) (the Clinger-Cohen Act); 44 USC 3601 (the Federal Information Security Management Act of 2002); Federal Preparedness Circular (FPC) 65; 10 USC 2224 (the National Defense Authorization Act for FY 2000); and Office of Management and Budget (OMB) Circular A–130. National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, is the basis of this document. AR 25-1, Army Knowledge Management and Information Technology Management, and AR 25-2, Information Assurance, require system owners to develop and test contingency plans.

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2 b.

"We recommend that the ...Chief Information Officer for the Department of the Army...Require that the Designated Approving Authority, the user representative, the program manager, and the Certifying Authority approve contingency plans for information systems."

Army comment:

Concur. Department of the Army will comply with ASD NII Contingency Planning policy and procedures when promulgated. As an interim measure, pending publication of specific DoD guidance, Army will supplement DA PAM 25-1-2 procedures with a Best Business Practice on Contingency Planning. For systems in the acquisition process, the User Representative, the Program Manager, the Certifying Authority and the Designated Approving Authority will be required to review, approve, and sign the Contingency Plan. Contingency Plans for Installation networks will be reviewed and approved by the Certification Authority and the Designated Approving Authority. The Contingency Planning Best Business Practice is under development and will be promulgated by 30 November 2007. System Owners will be required to review, update, and provide the Office of Information Assurance and Compliance with a signed Contingency Plan for each system under their control by 01 July 2008.

Recommendation 2c.

"We recommend that the ...Chief Information Officer for the Department of the Army...Require that system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006, and document results."

Army comment:

Concur. Existing Department of Army guidance in DA PAM 25-1-2 requires system owners to conduct recurring test of contingency plans under a variety of conditions that would require the activation of the Contingency Plan. This guidance includes testing of DoD Instruction 8500.2 security controls.

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2d (1):

"We recommend that the ...Chief Information Officer for the Department of the Army... Implement management controls to verify that system owners:
(1) Develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997 and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002."

Army comment:

Concur. Department of the Army guidance for the development of contingency plans is contained in DA PAM 25-1-2, Information Technology Contingency Planning, dated 16 November 2006. This is an official Department of the Army pamphlet that provides procedures for developing and exercising Information Technology contingency plans. This pamphlet supports AR 25–1 in implementing Title 10, United States Code, and Section 1401, Title 40, United States Code (Public Law 104–106, the Clinger-Cohen Act). DA PAM 25-1-2 is based on National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. The Army Portfolio Management Solution (APMS) is the official and authoritative source (data base of record) for information on all Army Information Technology systems that is submitted to the DITPR. Information in the APMS is submitted by the system owners and reviewed on a weekly basis by the Office of Information Assurance and Compliance to verify that system owners have developed contingency plans as required. System owners who are not in compliance are contacted, and required to provide a Plan of Action and Milestone to this office indicating when they will become compliant.

3

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2d (2):

"We recommend that the ...Chief Information Officer for the Department of the Army... Implement management controls to verify that system owners: (2) Conduct recurring tests of system contingency plans in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006."

Army comment:

Concur. Department of the Army guidance for the development of contingency plans is contained in DA PAM 25-1-2, Information Technology Contingency Planning, dated 16 November 2006. This is an official Department of the Army pamphlet that provides procedures for developing and exercising Information Technology contingency plans. This pamphlet supports AR 25–1 in implementing Title 10, United States Code, and Section 1401, Title 40, United States Code (Public Law 104–106, the Clinger-Cohen Act). DA PAM 25-1-2 is based on National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. The Army Portfolio Management Solution (APMS) is the official and authoritative source (database of record) for information on all Army Information Technology systems that is submitted to the DITPR. Information in the APMS is submitted by the system owners and reviewed on a weekly basis by the Office of Information Assurance and Compliance to verify that system owners have tested contingency plans at least annually as required. System owners that have outdated Contingency Plans are contacted and required to update their system entries in the APMS, and provide a Plan of Action and Milestones to the Office of Information Assurance and Compliance indicating when they will be compliant.

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2d (3):

"We recommend that the …Chief Information Officer for the Department of the Army…Implement management controls to verify that system owners: (3) Populate the "contingency plan" and "contingency plan last tested" data fields in the DoD Information Technology Portfolio Repository with complete and accurate system information."

Army comment:

Concur. Department of the Army guidance for the development of contingency plans is contained in DA PAM 25-1-2, Information Technology Contingency Planning, dated 16 November 2006. This is an official Department of the Army pamphlet that provides procedures for developing and exercising Information Technology contingency plans. This pamphlet supports AR 25–1 in implementing Title 10, United States Code, and Section 1401, Title 40, United States Code (Public Law 104–106, the Clinger-Cohen Act). DA PAM 25-1-2 is based on National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002. The Army Portfolio Management Solution (APMS) is the official and authoritative source (database of record) for information on all Army Information Technology systems that is submitted to the DITPR. Information in the APMS is submitted by the system owners and reviewed on a weekly basis by the Office of Information Assurance and Compliance to verify that system owners have tested contingency plans at least annually as required. System owners that have outdated Contingency Plans are contacted and directed to update their system entries in the APMS. At present, there is no independent method to verify the accuracy of the data entered by the system owners; under Recommendation 2b (above), Army will begin requiring System Owners to provide the Office of Information Assurance and Compliance with a copy of their authenticated Contingency Plan. Full implementation of Recommendation 2b by 01 July 2008 will only insure that a Contingency Plan exists. The Army Best Business Practice on Contingency Planning (Reference 2b) will require that System Owners of Mission-Critical systems submit a digitally signed message to the Office of Information Assurance and Compliance certifying that the Contingency Plan for their system has undergone annual testing. Copies of the message will be archived and maintained for inspection by Army Audit Agency and Army and DoD Inspectors General.

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2e:

"We recommend that the ...Chief Information Officer for the Department of the Army...Impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository."

Army comment:

Concur. The Army Chief Information Officer will impose appropriate sanctions, which may include holding of funds, withdrawal of Authority to Operate, or denial of network connectivity on system owners who do not adhere to Army Contingency Planning policy and procedures.

Recommendation 2f:

"We recommend that the ...Chief Information Officer for the Department of the Army...Implement automated controls, if applicable, on the Component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields."

Army Comment:

Concur. The Army system used to populate the DITPR is the Army Portfolio Management Solution (APMS), which is operated under strict configuration management. Engineering Change Proposals are being developed and will be presented to the APMS Configuration Control Board to comply with and implement this recommendation. These include making the Contingency Plan field a mandatory requirement which must be populated with an appropriate response (leaving the field blank will not be an acceptable response), and a means to cross check entries to prevent duplicate reporting. The time table for submitting the Engineering Change Proposals to the APMS CCB is 10 January 2008, with the implementation of changes to the APMS by 01 July 2008.

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2g:

"We recommend that the …Chief Information Officer for the Department of the Army…Prepare a Component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning."

Army comment:

Concur. An Army-level Plan of Action and Milestones will be developed and issued within 90 days of the issuance of the DoD IG's final report on Contingency Planning.

Recommendation 2h:

"We recommend that the …Chief Information Officer for the Department of the Army…Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report."

Army comment:

Concur. The Chief Information Officer will require system owners identified in this report to develop and submit to the Office of Information Assurance and Compliance, a Plan of Action and Milestones.

DEPARTMENT OF THE ARMY RESPONSE TO RECOMMENDATIONS AND ACTIONS TAKEN REGARDING DODIG DRAFT REPORT ON CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS (PROJECT NO. D2007-D000LB-0080.000)

Recommendation 2i:

"We recommend that the ...Chief Information Officer for the Department of the Army...Review assertions made in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems and interview the information assurance professionals to verify that the information in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum is accurate."

Army comment:

Concur. The Army is in the process of implementing and refining its automated controls used to validate entries in the Army Portfolio Management Solution (APMS).

Recommendation 2j:

"We recommend that the ...Chief Information Officer for the Department of the Army...Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement."

Army comment:

Concur. The Office of Information Assurance and Compliance conducted a review of the Army Portfolio Management Solution (APMS) to identify those systems that had indicated both Mission Critical and Mission Assurance Category III. As of 05 November 2007, there were 14 Mission Critical systems registered in the APMS as Mission Assurance Category III systems. The Office of Information Assurance and Compliance is contacting the system owners and requiring that they justify in writing the Mission Criticality assignment and Mission Assurance Category assignments. This issue will be worked through the Army Portfolio Management process. This action will be completed by 10 January 2008.

Department of the Navy Comments

DEPARTMENT OF THE NAVY
OFFICE OF THE CHIEF INFORMATION OFFICER
1000 NAVY PENTAGON
WASHINGTON, DC 20350-1000

2 November 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

Subj: RESPONSE TO DOD-IG DRAFT REPORT "CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS" (PROJECT NO. D2007-D000LB-0080.000 OF 2 OCTOBER 2007)

Ref: (a) DoD-IG memo of 2 Oct 07

Reference (a) requested Department of the Navy (DON) response by 2 November 2007 to the subject draft audit report. The following comments apply:

We concur with the findings of the audit.

The DON Chief Information Officer (CIO) submits the following comments and action to be taken on the Department of Defense Inspector General's (DoD-IG) recommendations:

1. DoD-IG Recommendation One is addressed to the Assistant Secretary of Defense for Network and Information Integration (ASD (NII))/DoD CIO. The ASD(NII)/DoD CIO will respond to this recommendation.

2. DoD-IG Recommendation Two is addressed to ASD (NII) and Component Chief Information Officers (CIOs). HQMC response is attached in enclosure (1).

   a. Require that system owners develop contingency plans in accordance with DoD Instruction (DoDI) 5200.40 (DoD Information Technology (IT) Certification and Accreditation Process - DITSCAP) and NIST Special Publication 800-34.

   Concur; DON CIO will issue specific guidance on this subject after receipt of the final audit report.

   b. Require that the Designated Approving Authority, user representative, program manager, and Certifying Authority approve contingency plans for information systems.

   Concur in principle, in that DON CIO will issue guidance regarding approval for contingency plans after receipt of the final audit report.

   c. Require that system owners conduct recurring tests of contingency plans under realistic conditions.

   Concur; DON CIO will issue specific guidance on this subject after receipt of the final audit report.

d. Implement management controls to verify that system owners (1) develop contingency plans in accordance with DITSCAP and NIST Special Publication 800-34, (2) conduct recurring tests of system contingency plans in accordance with DoDI 8500.2 (Information Assurance Implementation) and the FISMA legislation, and (3) populate the "contingency plan" and "contingency plan last tested" fields in DITPR DON.

Concur; DON CIO will issue specific guidance on this subject after receipt of the final audit report, and already has part (3) underway.

e. Impose sanctions on system owners who do not prepare and test their systems' contingency plans, or supply complete, accurate, and authoritative information in DITPR-DON.

Concur; DON CIO will issue specific guidance on this subject after receipt of the final audit report.

f. Implement automated controls, if applicable, on DITPR-DON that are used to populate DITPR to prevent blank data fields, duplicate reporting of system and system information, and reporting of different information for similar data fields.

Concur with the requirement; however, DON CIO and OSD are studying this recommendation and the feasibility of automated controls. DON CIO is accomplishing these reviews manually approximately bi-monthly, and reporting results to DON Echelon II/Major Subordinate Commands for their action.

g. Prepare a Component-level POA&M, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

Concur; DON CIO will develop a Component level POA&M.

h. Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a POA&M within 90 days of the issuance of the final version of this report.

Concur; DON CIO will issue specific guidance after receipt of the final audit report.

i. Review assertions made in the DITPR CIO memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems. Interview the IA professionals to verify that the information in the DITPR CIO memorandum is accurate.

Subj: RESPONSE TO DOD-IG DRAFT REPORT "CONTINGENCY PLANNING FOR DOD MISSION-CRITICAL INFORMATION SYSTEMS" (PROJECT NO. D2007-D000LB-0080.000 OF 2 OCTOBER 2007)

Concur with the requirement; however, DON CIO and OSD are studying this recommendation and the feasibility of automated controls. DON CIO will issue specific guidance on the interview portion of this recommendation after receipt of the final audit report.

j. Review any system designated as mission critical and MAC-III to identify the rationale for the designation. Require that owners document the rationale in the SSAA.

Concur; DON CIO will issue specific guidance on this subject after receipt of the final audit report.

The DON CIO points of contact for this audit are James Collins (703-602-6202, james.e.collins.ctr@navy.mil) and Jennifer Ellett (703-602-6110, jennifer.ellett.ctr@navy.mil).

John J. Lussier
Deputy Chief Information Officer for
Policy and Integration and
DON Senior IA Official

Copy to:
ASD (NII) (Attn: John Hunter)
NAVIG (Attn: Juanita Gilbert)
CNO (N61)
CMC (C4/IA)

3

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
WASHINGTON DC

OFFICE OF THE SECRETARY

NOV 0 5 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE OFFICE OF INSPECTOR GENERAL

FROM: SAF/XC
1800 Air Force Pentagon
Washington DC 20330-1800

SUBJECT: Air Force Response to DoDIG Report on Contingency Planning for DoD Mission-Critical Information Systems (Project No. D2007-D000LB-0080.000)

Thank you for the opportunity to review and comment on the subject report. The Air Force plans to use the annual Information Technology (IT) investment review and certification process to ensure contingency plans are developed and tested. Additionally, our Security, Interoperability, Sustainability, Supportability, and Usability (SISSU) process will ensure compliance with DoD Instruction 8500.2. An Air Force response to each of the DoD IG audit findings is provided below.

DoD IG Comments on Preparing Contingency Plans: 68 of 85 the Air Force's mission-critical systems sampled did not develop or could not provide evidence of a contingency plan.

Air Force Response to Report Findings: A detailed instruction on contingency plan development was included in the Air Force FY07 FISMA Reporting Guidance released by the AF CIO on 17 April 2007. System owners were directed to use the NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, to develop and maintain a viable contingency planning program. The Air Force will incorporate contingency planning procedures outlined in NIST SP 800-34 into Air Force policy.

DoD IG Comments on Testing Contingency Plans: None of the 85 systems sampled could provide evidence of testing the contingency plan.

Air Force Response to Report Findings: A detailed instruction on contingency plan testing, training, and exercises was included in the Air Force FY07 FISMA Reporting Guidance released by the AF CIO on 17 April 2007. As noted above, contingency plan development and testing will be audited to ensure gaps are identified, training is relevant, recovery personnel are prepared, and exercises are conducted and documented to improve plan effectiveness.

The Air Force point of contact for this report is Mr. Kenneth Brodie, 703-696-7557, kenneth.brodie@pentagon.af.mil.

MICHAEL W. PETERSON, Lt Gen, USAF
Chief of Warfighting Integration and
Chief Information Officer

U.S Transportation Command Comments

UNITED STATES TRANSPORTATION COMMAND
508 SCOTT DRIVE
SCOTT AIR FORCE BASE, ILLINOIS 62225-5357

NOV 13 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

FROM: TCJ8

SUBJECT: Review of Draft DOD Inspector General Report, Contingency Planning for DOD Mission-Critical Information Systems, Project No. D2007-D000LB-0080.000, 2 October 2007

1. USTRANSCOM has reviewed the subject draft report and notes the identified results reflect very favorably on our command when compared to other sampled Combatant Command, Service and Agency (CC/S/A) systems. The audit states 13 of 14 USTRANSCOM systems reviewed maintained compliant contingency plans. In summary, the report indicates the Core Automated Maintenance System –For Mobility (CAMS-FM) did not provide a DOD compliant contingency plan and eight of the 14 USTRANSCOM system owners did not correctly report the date of the last test of the system's contingency plan in DOD Information Technology Portfolio Registry (DITPR).

2. For the purpose of clarification, we offer the following for your consideration:

a. Thirteen of the 14 USTRANSCOM systems sampled maintained a compliant contingency plan. This is largely attributable to mature and effective Chief Information Officer (CIO) and portfolio management controls. The contingency plan for the one system judged to be no-compliant (CAMS-FM, reference DITPR ID 349) was somewhat complicated by collateral agreements required to perform failover operations between Defense Information Systems Agency (DISA) - Oklahoma City, and DISA – St. Louis. Those agreements are now secure and the associated contingency plan has been updated. We subsequently tested the contingency plan in July 2007 and found it to be effective and compliant.

b. We believe six of the eight flagged systems had compliant contingency plan test dates in the DITPR at the time the sample was taken. The two remaining systems were tested within guidelines and contingency plan test dates entered in DITPR within four weeks of compliance requirements. We attribute the reporting/update latency to Federal Information Security Management Act (FISMA) and DITPR guidelines allowing for a 30-day update cycle following contingency plan testing. USTRANSCOM system contingency testing information is posted in DITPR within one week of receiving the signed system contingency plan exercise result documentation.

3. USTRANSCOM continues to emphasize and maintain strong CIO and Information Technology (IT) portfolio management Controls. DODI 8500.2 serves as the basis for USTRANSCOM Information Assurance (IA) implementation policy and annual/semi-annual testing requirements are strictly enforced. USTRANSCOM has developed and standardized templates to assist system managers in developing contingency plans and documenting

Printed on recycled paper

contingency plan results. These templates are based on DODI 8500.2, FISMA guidance, and lessons learned from the DODIG audit. Finally, USTRANSCOM requested and received Plans of Actions Milestones (POA&Ms) from systems managers following the last audit of DITPR contingency plan data in January 2007. USTRANSCOM continuously monitors the POA&Ms and sends update requests to system managers on a monthly basis. When the system managers submit inadequate documentation, the USTRANSCOM CIO support staff and subject matter experts assist the system managers in achieving compliance as part of the formalized USTRANSCOM CIO Program Review Process.

4. The USTRANSCOM POC is Ms Rose Wesolowski, TCJ8-A, DSN 779-5038, Commercial 618-229-5038, or email rose.wesolowski@ustranscom.mil.

ALAN K. BENTLEY
Director, Program Analysis
and Financial Management

cc:
TCIG
TCJ6
TCCS

Defense Contract Management Agency Comments

DEFENSE CONTRACT MANAGEMENT AGENCY
6350 WALKER LANE, SUITE 300
ALEXANDRIA, VIRGINIA 22310-3226

IN REPLY REFER TO DCMA-DMI

NOV 19 2007

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL
FOR READINESS AND OPERATIONS SUPPORT

SUBJECT: DODIG Draft Report on Contingency Planning for DoD Mission-Critical Information Systems

Reference DODIG draft audit report, Project No. D2007-D000LB-0080.

We have attached the Headquarters, Defense Contract Management Agency response to recommendation 2 in the subject audit report.

Point of contact is Ms. Sonya Moman at 703-428-1465 or sonya.moman@dcma.mil.

Keith D Ernst

KEITH D. ERNST
Acting Director

FINDING: The information in the DoD Information Technology Portfolio Repository (DITPR) on contingency planning is not reliable on the basis of sample results.

DCMA Response: All our systems do have contingency plans, and they are all tested periodically, including Sampled System 208/DITPR Identification Number 423, which is the Mechanization of Contract Administration Services (MOCAS) system. DCMA shares ownership of MOCAS with the Defense Finance and Accounting Service (DFAS), and the Defense Information Systems Agency (DISA) hosts and operates MOCAS at their Defense Electronic Computing Center (DECC) Ogden for DCMA and DFAS on a reimbursable basis. DISA has prepared a contingency plan for all applications hosted by DECC Ogden. We and DFAS participate in the testing of that plan as it relates to MOCAS.

While the MOCAS contingency plan testing date in DITPR at the time of the initial IG data pull in January 2007 was incorrect (the entered date was actually a date we tested our contingency plan for our eTools suite of applications), we entered the correct date on May 15, 2007 and promptly informed the IG's office of that correction. DITPR now contains the date of the latest test of the MOCAS contingency plan, June 29, 2007.

RECOMMENDATION 2: We [DoD IG] recommend that … the Chief Information Officers for … the Defense Contract Management Agency [among multiple other DoD Components] …:

a. Require that system owners develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy.

   DCMA Response: Partially Concur. The DoD CIO by memorandum dated July 6, 2006, subject: Interim Department of Defense (DoD) Information Assurance (IA) Certification and Accreditation Process Guidance, instructed all DoD personnel to disregard DoD Instruction 5200.40 and comply with the requirements of draft DoD Instruction 8510.bb. Additionally, as noted above in our response under Finding, DECC Ogden hosts MOCAS along with multiple other DoD systems. DECC Ogden has prepared a contingency plan for all the applications that it hosts. That is appropriate, as neither DCMA nor DFAS have mainframe computing resources that could be used as contingency MOCAS backup resources, but DISA does. DECC Ogden's backup site is in fact another DECC.

b. Require that the Designated Approving Authority, the user representative, the program manager, and the Certifying Authority approve contingency plans for information systems.

   DCMA Response: Partially Concur. We believe that approval authority for contingency plans that will necessarily involve the use of DISA resources, as is the case for DISA-hosted applications such as MOCAS, properly resides within DISA. We do believe, though, that there should always be robust dialog between DISA and all the relevant system certification and accreditation Designated Approving Authorities (which for MOCAS is the

DCMA CIO), and user representatives (which for MOCAS are from both DCMA and DFAS), et al, about the contingency plan contents and the tests thereof. Such robust dialog is in fact the norm with respect to MOCAS contingency planning and testing.

c. Require that the system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoD Instruction 8500.2, Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DOD Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006, and document results.

DCMA Response: Concur. Tests of the MOCAS contingency plan are conducted annually. (The latest was in fact conducted in June 2007.) After Action Reports are published after each test, with observations and recommendations for further improvements.

d. Implement management controls to verify that system owners:

(1) Develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997 and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

(2) Conduct recurring tests of system contingency plans in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006

(3) Populate the "contingency plan" and "contingency plan last tested" data fields in the DoD Information Technology Portfolio Repository with complete and accurate system information.

DCMA Response: Concur--although, as we noted above, the DoD CIO has instructed all DoD personnel to disregard DoD Instruction 5200.40 and comply with draft DoD Instruction 8510.bb.

e. Impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository.

DCMA Response: Partially Concur. We do not believe that there should be a mandatory requirement to impose sanctions in all instances. For example, it should not be imposed for isolated instances where an individual inadvertently enters incorrect data. In such instances, non-disciplinary corrective action is appropriate. Conversely, disciplinary action may well be appropriate for willful or flagrantly negligent non-compliances. Accordingly, we believe the recommendation should be rewritten to include both disciplinary and non-disciplinary corrective action. For example, it might state; "Impose appropriate disciplinary or other corrective action in instances

where system owners do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository."

f. Implement automated controls, if applicable, on the Component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields.

DCMA Response: Partially Concur. DCMA does not use an automated system to populate the DITPR. A DCMA Information Assurance professional performs manual updates which are reviewed by the DCMA Deputy CIO.

g. Prepare a Component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

DCMA Response: Partially Concur. This recommendation is not applicable to DCMA since there are no extant security weaknesses related to contingency planning.

h. Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report.

DCMA Response: Partially Concur. This recommendation is not applicable to DCMA as the only DCMA system identified during the DoD IG review as having a weakness was MOCAS, and there is now a compliant MOCAS contingency plan in place and it is being tested annually.

i. Review assertions made in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems. Interview the information assurance professionals to verify that the information in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum is accurate.

DCMA Response: Concur. We have completed a review of DCMA information in DITPR information and have verified that it is accurate.

j. Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement.

DCMA Response: Partially concur. This recommendation is not applicable to DCMA as we have no mission critical systems designated as Mission Assurance Category III.

Defense Information Systems Agency Comments

DEFENSE INFORMATION SYSTEMS AGENCY
P.O Box 4502
ARLINGTON, VIRGINIA 22204-4502

IN REPLY REFER TO: Chief Information Officer (SPI)

2 NOV 200

MEMORANDUM FOR ASSISTANT INSPECTOR GENERAL FOR READINESS AND OPERATIONS SUPPORT

SUBJECT: DISA Response to the Report Findings and Recommendations

1. In accordance with DoD Directive 7650.3, our response to the recommendations presented in the DoD IG report, "Contingency Planning for DoD Mission-Critical Information Systems (Project No. D2007-D000LB-0080.000) is indicated in the Attachment 1 enclosed with this correspondence.

2. We recognize that comprehensive guidance and control measures can better the effort to have Components supply complete, accurate, and authoritative data into the DoD Information Technology Portfolio Repository (DITPR). I am confident that the corrective processes initiated in March 2007 are properly focused to improve our DITPR FISMA input.

3. My point of contact for additional information is Greg Parma, (703) 681-2112, DSN 761, or through email at greg.parma@disa.mil, or Kunal Johar, (703) 681-2117, DSN 761, at kunal.johar@disa.mil.

JOHN J. GARING
Chief Information Officer

1 Enclosure:
Attachment 1 - DISA Response To Recommendations

Attachment 1 – DISA Response To Recommendation 2

a. Require that system owners develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy.

DISA utilizes the annual DoD FISMA guidance which requires all systems to have a contingency plan developed and tested according to the DODI 8500.2 controls. At the minimum this contingency plan must be tested once per year.

b. Require that the Designated Approving Authority, the user representative, the program manager, and the Certifying Authority approve contingency plans for information systems.

DISA's certification and accreditation process requires the DAA, user representative, program manager, and the certifying authority to review and approve the SSAA as indicated by the DITSCAP.

As a part of the newly released DISAI 630-230-19 DISA enforces the requirement. The implementation manual to be released July 2008 will require the contingency plan to be reviewed before the SSAA can be approved by the four stake holders identified.

c. Require that system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006, and document results.

As a part of the newly released DISAI 630-230-19 DISA enforces the requirement. The implementation manual to be released July 2008 will address the specific procedures to ensure contingency plan compliance. Currently guidance is provided to Information Assurance Managers and Program managers via a DISA wide FISMA portal hosted on the Defense Online system. The current guidance has been adapted from procedures the annual DoD FISMA guidance.

d. Implement management controls to verify that system owners:

(1) Develop contingency plans in accordance with DoD Instruction 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997 and the National Institute of Standards and Technology Special Publication 800-34"Contingency Planning Guide for Information Technology Systems," June 2002.

(2) Conduct recurring tests of system contingency plans in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal

Attachment 1 – DISA Response To Recommendation 2

Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006.

(3) Populate the "contingency plan" and "contingency plan last tested" data fields in the DoD Information Technology Portfolio Repository with complete and accurate system information.

Beginning February 2007, DISA has instated monthly reporting requirements for the directorates throughout the agency. Each month the directorates are notified of systems currently out of compliance as well as with a timeline for future system compliance expiration dates. DISA has developed an in-house automated tool to provide oversight on this information. This tool has been shared with the Air Force and the Navy FISMA leads.

e. Impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository.

The DISA Senior Information Assurance Officer has the authority to issue a notice for denial of authority to operate for a system that presents a threat to the security of the network.

This process will be used to enforce compliance of system contingency plan testing.

f. Implement automated controls, if applicable, on the Component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields.

DISA PEO-IAN is currently evaluating automated IA management tools for fielding DoD-wide. In the interim, the DISA Office of the CIO is using an automated DITPR compliance tracking tool to ensure the data quality of FISMA related fields.

g. Prepare a Component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

Within 90 days of the issuance of the final report, the DISA Office of the CIO will provide a plan of action and milestones to ensure the mission critical systems have complied with contingency planning requirements.

The DISA Office of the CIO will increase the oversight role of documentation compliance in its functional processes.

Attachment 1 – DISA Response To Recommendation 2

h. Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report.

As per recommendation g, the DISA CIO will require system owners to submit a plan of action and milestones to ensure their systems are complaint with regards to contingency planning within 90 days of the issuance of this final report.

i. Review assertions made in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems. Interview the information assurance professionals to verify that the information in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum is accurate.

DISA Office of the CIO is using an automated DITPR compliance tracking tool to ensure the data quality of FISMA related fields. DISA will expand this tool to assist with the compliance tracking of non-FISMA DITPR tracked fields.

j. Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement.

Within 90 days of the issuance of the final report DISA CIO will review all MAC III systems designated as mission critical. Rationale will be documented and reviewed and if necessary systems will be reclassified.

Defense Logistics Agency Comments

Final Report Reference

DEFENSE LOGISTICS AGENCY
HEADQUARTERS
8725 JOHN J. KINGMAN ROAD
FORT BELVOIR, VIRGINIA 22060-6221

IN REPLY REFER TO J-65

NOV 19 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Report on Contingency Planning for DOD Mission Critical Information Systems (Project No. D2007-D000LB-0800.000)

The Defense Logistics Agency (DLA) has reviewed the draft report and concurs with the recommendations provided in paragraph 2 except as suggested for paragraph 2b. We recommend that paragraph 2b be modified to allow the Designated Approving Authority or an authorized representative to approve contingency plans for information systems.

Additionally, we have updated the data in Appendix B for DLA's systems tested this year and included it at Attachment 1. We are pleased to highlight that the system with the 2003 test date was decommissioned this year and that the remaining DLA systems are current, with the next contingency plan test dates due during calendar year 2008.

Attachment 1 Omitted

The point of contact is Mr. Miles Holtzman, J-651, (703) 767-6916, e-mail: miles.holtzman@dla.mil. All administrative queries should be addressed to Mr. Clarence McNeill, J-651, (703) 767-2181, e-mail: clarence.mcneill@dla.mil.

MAE DE VINCENTIS
Director, Information Operations
Chief Information Officer

Attachment

~~FOR OFFICIAL USE ONLY~~

Federal Recycling Program Printed on Recycled Paper

Defense Threat Reduction Agency Comments

Defense Threat Reduction Agency
8725 John J. Kingman Road MSC 6201
Ft Belvoir, VA 22060-6201

NOV 01 2007

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

SUBJECT: Defense Threat Reduction Agency (DTRA) Chief Information Officer (CIO) Response to the Department of Defense Office of the Inspector General Draft Report Project No. D2007-D000LB-0080.000, "Contingency Planning for DoD Mission Critical Information Systems," dated October 2, 2007

The Office of the DTRA CIO appreciates the opportunity to comment on the draft DoD IG Report Project No. D2007-D000LB-0080.000, "Contingency Planning for DoD Mission Critical Information Systems."

This Office believes the draft report accurately reflects the state of the Department of Defense Information Technology Portfolio Repository (DITPR) in January 2007 and provides workable recommendations that will facilitate the remediation of the noted deficiencies. It should be noted that this Agency has focused its efforts and resources to improve DTRA data quality and integrity in DITPR. Specific comments on the recommendations in the draft report are provided in the attachment.

The Action Officer is Mr. Rob Bleck. He may be reached at (703) 767-7840 (DSN 427-7840) or Rob.Bleck@dtra.mil.

David G. Belva
Chief Information Officer

DoD IG Draft Report dated October 2, 2007
Project No. D2007-D000LB-0080.000

"Contingency Planning for DoD Mission Critical Information Systems"

DEFENSE THREAT REDUCTION AGENCY COMMENTS
TO THE DOD IG RECOMMENDATIONS

RECOMMENDATION 1a: The DoD IG recommends that the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer (ASD (NII)/CIO) require DoD Components to use the National Institute of Standards and Technology (NIST) Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, when developing and testing DoD contingency plans, or issue a comprehensive DoD contingency planning policy.

DTRA RESPONSE: Concur. The lack of specific detailed DoD guidance about contingency planning impedes DTRA's ability to develop, test, and approve contingency plans for information systems.

RECOMMENDATION 1b: The DoD IG recommends that the ASD (NII)/CIO inform the Office of Management and Budget and Congress that DoD does not have internal controls over the accuracy of data on the security of its information technology systems, and include a caveat to that effect in all reports based on data drawn from the DoD Information Technology Portfolio Repository (DITPR) until demonstrably effective internal controls have been in place for at least 1 full year.

DTRA RESPONSE: Defer to ASD (NII)/CIO.

RECOMMENDATION 1c: The DoD IG recommends that the ASD (NII)/CIO immediately issue a supplement to the DoD CIO Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) for Fiscal Year 2007 (FY07)," May 21, 2007, and all continuations of the guidance, that contains information on testing contingency plans that was included in the supplemental section of the DoD CIO Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006.

DTRA RESPONSE: Concur. DTRA staff would benefit from the future inclusion of the information on testing contingency plans contained in Attachment 4, Supplementary Information: Completion of DITPR and IT Registry FISMA Fields, to the FISMA Guidance for FY 06.

RECOMMENDATION 1d: The DoD IG recommends that the ASD (NII)/CIO immediately issue a supplement to the DoD CIO Memorandum, "Department of Defense (DoD) Information Technology (IT) Portfolio Repository (DITPR) and DoD SECRET Internet Protocol Router Network (SIPRNET) IT Registry Guidance for 2007-2008," September 6, 2007, and all continuations of the guidance that:

(1) Defines an automated control and specifies the types of data integrity rules DoD Components must implement to ensure they supply complete, accurate, and authoritative data in the DITPR.

(2) Clarifies the difference between a contingency plan and a continuity of operations plan.

(3) Removes reference to continuity of operations plans in the "contingency plan" and "contingency plan last exercised" data fields in the DITPR and the DITPR Data Dictionary.

DTRA RESPONSE: Concur. Issuance of the recommended supplement would assist DTRA to improve its data quality and integrity. Clarification of definitions should eliminate the inappropriate substitution of one term for the other. Removal of the continuity of operations plans reference would lead to more accurate reporting of contingency plan existence and testing in DITPR.

RECOMMENDATION 1e: The DoD IG recommends that the ASD (NII)/CIO implement a training program in contingency planning for DoD Component officials who develop, test, and approve contingency plans for information systems.

DTRA RESPONSE: Concur. Implementation of such a training program would benefit DTRA by developing a cadre of individuals with the requisite skills to more expeditiously complete Component contingency planning.

RECOMMENDATION 2a: The DoD IG recommends that the ASD (NII)/CIO; the Director, Business Transformation Agency (BTA); and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the Defense Contract Management Agency (DCMA), the Defense Threat Reduction Agency (DTRA), the Defense Information Systems Agency (DISA), the Defense Logistics Agency (DLA), the Missile Defense Agency (MDA), and the TRICARE Management Activity (TMA) require that system owners develop contingency plans in accordance with DoD Instruction (DoDI) 5200.40, "DoD Information Technology Certification and Accreditation Process (DITSCAP)," December 30, 1997, and the NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy.

DTRA RESPONSE: Partially concur. It should be noted that the DITSCAP does not tell how to write or test a contingency plan, nor does its replacement the DoD Information Assurance Certification and Accreditation Process (DIACAP). DITSCAP required and DIACAP requires contingency planning and testing of contingency plans. There is no current DoD issuance that states exactly what should be in a contingency plan or how to test it. NIST 800-34 provides a detailed description of how to write a contingency plan, explains how contingency planning fits into the system development life cycle and risk management, and provides a template. Contingency plans should be developed in accordance with the NIST 800-34 until DoD issues a formal contingency planning policy.

RECOMMENDATION 2b: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA require that the Designated Approving Authority, the user representative, the program manager, and the Certifying Authority approve contingency plans for information systems.

DTRA RESPONSE: Partially concur. The current practice at DTRA requires the Designated Approving Authority, the program manager, and the Certifying Authority approve contingency plans for information systems. Because it is extremely difficult to find someone without a vested interest in the system to perform the user representative functions defined in DIACAP, the user representative role in approval of information system contingency plans should be optional.

RECOMMENDATION 2c: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA require that system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD CIO Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006, and document results.

DTRA RESPONSE: Nonconcur. Resource constraints prevent recurring tests of contingency plans under realistic conditions. Desktop testing is economical and, if done properly, can be thorough enough to identify security weaknesses.

RECOMMENDATION 2d: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA implement management controls to verify that system owners:

(1) Develop contingency plans in accordance with DoDI 5200.40, "DITSCAP," December 30, 1997 and the NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

(2) Conduct recurring tests of system contingency plans in accordance with DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and DoD CIO Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006 (FY 06)," April 4, 2006.

(3) Populate the "contingency plan" and "contingency plan last tested" data fields in the DITPR with complete and accurate system information.

DTRA RESPONSE: Partially concur. Contingency plans should be developed in accordance with the DIACAP-replacement for DoDI 5200.40 and should be tested annually.

RECOMMENDATION 2e: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DITPR.

DTRA RESPONSE: Concur-in-principle. It is first necessary to determine meaningful sanctions that will not compromise operational effectiveness or mission achievement.

RECOMMENDATION 2f: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA implement automated controls, if applicable, on the Component system used to populate the DITPR to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields.

DTRA RESPONSE: Concur-in-principle. Although DTRA does not have a Component system used to populate the DITPR, DTRA plans to implement automated controls using its certification and accreditation database to validate downloaded DITPR data.

RECOMMENDATION 2g: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA prepare a Component-level Plan of Action and Milestones (POA&M), within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

DTRA RESPONSE: Concur-in-principle. DTRA prepared and submitted a Component-level POA&M in conjunction with its Fiscal Year 2007 FISMA Report, which addresses security weaknesses in contingency planning for its reported systems.

RECOMMENDATION 2h: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA require that owners of systems identified in this report as having security weaknesses in contingency planning develop a POA&M within 90 days of the issuance of the final version of this report.

DTRA RESPONSE: Concur-in-principle. DTRA has initiated action to address security weaknesses in contingency planning through individual system POA&Ms.

RECOMMENDATION 2i: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the

Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA review assertions made in the DITPR CIO Memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems. Interview the information assurance professionals to verify that the information in the DITPR CIO Memorandum is accurate.

DTRA RESPONSE: Concur-in-principle. Recommended action by the DoD IG is current practice at DTRA.

RECOMMENDATION 2j: The DoD IG recommends that the ASD (NII)/CIO; the Director, BTA; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the DCMA, the DTRA, the DISA, the DLA, the MDA, and the TMA review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement.

DTRA RESPONSE: Partially concur. The rationale should be documented in the System Information Security Plan as required by the DIACAP.

Missile Defense Agency Comments

DEPARTMENT OF DEFENSE
MISSILE DEFENSE AGENCY
7100 DEFENSE PENTAGON
WASHINGTON, DC 20301–7100

DOB

OCT 29 2007

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

SUBJECT: Response to Draft Report of "Contingency Planning for DoD Mission Critical Information Systems," Project No. D2007-D000LB-0080.000

The Missile Defense Agency appreciates the opportunity to review and ensure the subject Draft Report is factually accurate and to provide comments. The Agency has reviewed the Draft Report and concurs without comment. My point of contact for the subject Draft Report is Mr. Mirza Baig, Assistant Director, Program Liaison at (703) 692-6538.

PATRICIA SANDERS
Executive Director

TRICARE Management Activity Comments

THE ASSISTANT SECRETARY OF DEFENSE
1200 DEFENSE PENTAGON
WASHINGTON, DC 20301-1200

HEALTH AFFAIRS

NOV 1 2007

Ms. Kimberley Caprio
Office of the Inspector General
Department of Defense
400 Army Navy Drive
Arlington, VA 22202-4704

Dear Ms. Caprio:

This is the Office of the Assistant Secretary of Defense (Health Affairs)/ TRICARE Management Activity (TMA) response to the draft Department of Defense (DoD) Inspector General (IG) audit report, "Contingency Planning for DoD Mission-Critical Information Systems" (Project No. D2007-D000LB-0080.000)."

TMA acknowledges receipt of the draft audit report and concurs with the overall findings. TMA was pleased that the DoD IG singled out TRICARE for issuing contingency planning guidance and implementing automated controls to improve the overall management of the Military Health System (MHS) information assurance program.

TMA concurs with the recommendation that the Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer update and/or issue related Contingency Planning policies and guidance, processes, and management controls. TMA will ensure compliance with these efforts, update implementing policies and procedures, and incorporate DoD IG recommendations into the MHS Information Assurance Program.

Enclosed are comments to the recommendations in the final report. Please feel free to direct questions on this matter to Ms. Lois Kellett, at (703) 681-8836, or Mr. Gunther Zimmerman (Government Accountability Office IG Liaison), at (703) 681-3492.

Sincerely,

S. Ward Casscells, MD

Enclosure:
As stated

DEPARTMENT OF DEFENSE INSPECTOR GENERAL
DRAFT REPORT, DATED OCTOBER 2, 2007
D2007-D000LB-0080.000

Agency Comments on Draft Report, "Contingency Planning for Department of Defense Mission-Critical Information Systems"

DEPARTMENT OF DEFENSE COMMENTS

Recommendation 2: We recommend that the Assistant Secretary of Defense (Network and Information Integration)/Department of Defense (DoD) Chief Information Officer (CIO); the Director, Business Transformation Agency; and the CIOs for the Department of the Army, Department of the Navy, Department of the Air Force, the U.S. Strategic Command, the U.S. Transportation Command, the Defense Contract Management Agency, the Defense Threat Reduction Agency, the Defense Information System Agency, the Defense Logistics Agency, the Missile Defense Agency and the TRICARE Management Activity commit to the following:

a. Require that system owners develop contingency plans in accordance with DoD Instruction (DoDI) 5200.40, "DoD Information Technology Certification and Accreditation Process," December 30, 1997, and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002, until DoD issues formal contingency planning policy.

b. Require that the Designated Approving Authority, the user representative, the program manager, and the Certifying Authority approve contingency plans for information systems.

c. Require that system owners conduct recurring tests of contingency plans under realistic conditions and in accordance with DoDI 8500.2, "Information Assurance Implementation," February 6, 2003, and DoD CIO Memorandum, "Department of Defense Federal Information Security Management Act Guidance for Fiscal Year 2006," April 4, 2006, and document results.

d. Implement management controls to verify that system owners:

(1) Develop contingency plans in accordance with DoDI 5200.40, "DoD Information Technology Certification and Accreditation Process," December 30, 1997 and the National Institute of Standards and Technology Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002.

(2) Conduct recurring tests of system contingency plans in accordance with DoDI 8500.2, "Information Assurance Implementation," February 6, 2003, and DoD CIO

Memorandum, "Department of Defense Federal Information Security Management Act Guidance for Fiscal Year 2006," April 4, 2006.

(3) Populate the "contingency plan" and "contingency plan last tested" data fields in the DoD Information Technology Portfolio Repository with complete and accurate system information.

e. Impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository.

f. Implement automated controls, if applicable, on the component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate reporting of systems and system information, and reporting of different information for similar data fields.

g. Prepare a component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

h. Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report.

i. Review assertions made in the DoD Information Technology Portfolio Repository CIO Memorandum, including whether the component implemented automated controls and certify to only the current state of the security status for the components' information systems. Interview the information assurance professional to verify that the information in the DoD Information Technology Portfolio Repository CIO Memorandum is accurate.

j. Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement.

MHS Response: Concur. The DoD IG recommended that the Assistant Secretary of Defense (Network and Information Integration)/DoD CIO update and/or issue related Contingency Planning policies and guidance, processes, and management controls. The Military Health System (MHS) will ensure compliance with these efforts, update implementing policies and procedures, and incorporate DoD IG recommendations into the MHS Information Assurance Program.

U.S. Marine Corps Comments

DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
2 NAVY ANNEX
WASHINGTON, DC 20380-1775

IN REPLY REFER TO:
5500
C4/IA
26 Oct 2007

From: Brigadier General G. J. Allen, Director, HQMC Command, Control, Communications, and Computers
To: Department of Defense Inspector General
Via: Department of the Navy, Chief Information Officer

Ref: DEPARTMENT OF DEFENSE DRAFT REPORT DATED OCTOBER 2,2007; PROJECT NUMBER D2007-DOOOLB-0080.000

Subj: RESPONSE TO DEPARTMENT OF DEFENSE DRAFT REPORT DATED OCTOBER 2,2007; PROJECT NUMBER D2007-DOOOLB-0080.000

Purpose: To describe the Marine Corps enclave approach to reporting compliance with FISMA requirements and describe how the Marine Corps will comply with the DoD IG recommendations contained in the reference.

1. The Marine Corps has taken an enclave approach to meet Information Assurance reporting requirements. In September 2005, the Senior Information Assurance Official and Marine Corps Enterprise Network (MCEN) Designated Accrediting Authority (DAA) identified three enclaves that comprise the MCEN. The three enclaves are the Marine Corps SIPRNet, Marine Corps NIPRNet, and the Marine Corps Community of Interest (COI) of the Navy-Marine Corps Intranet (NMCI). These enclaves include all garrison and tactical information systems and networks located in or on Marine Corps bases, posts, camps, stations, and Major Subordinate Commands (MSCs). All networks, networked systems, and other information systems that are certified and accredited to operate within the MCEN are identified as belonging to one or more of the three enclaves and are identified as such in the approved enclave System Security Authorization Agreement (SSAA).

The enclave approach to meet Information Assurance requirements enables information systems within each enclave and operated at local levels to inherit characteristics and attributes of both the enclave and local site. For example, information system " X is identified as belonging to the MCEN NIPRNet enclave and is installed and operated at Camp Lejeune. This system is subject to the common configurations of the MCEN NIPRNet enclave as well as additional common configurations of Camp Lejeune. This means that the overarching Continuity of Operations Plan (COOP) and Contingency Plans (CP) associated with the MCEN NIRPNet apply, as well as the Camp Lejeune, site specific, COOP and CPs. We define this as a security inheritance. The system inherits the standards of the overarching network protections, and the local additional protections.

2. The following are the Marine Corps responses to audit findings:

a. Preparing Contingency Plans. The DoD IG projected that, based on sample results, evidence of CPs could not be provided for 100% of the Marine Corps information systems.

(1) The Marine Corps concurs with this finding.

(2) The Marine Corps will demonstrate system accountability in the POA&M following the enclave approach to IA requirements. The systems subject to audit by the DoD IG were assigned to one or more of the three enclaves and implemented at locations throughout the Marine Corps. COOP/CP documentation was provided for enclaves, as well as base/post/station/camp locations throughout the Marine Corps.

b. Contingency Plan Testing. The audit projected that, based on sample results, no CP tests were conducted or no evidence could be provided.

(1) The Marine Corps concurs with this finding.

(2) While the initial submission of test and after action reports did not explicitly identify the systems in question, the documentation showed an active contingency plan testing program. It is recognized that there is one region in the Marine Corps that had limited artifacts, and this was acknowledged early in the audit as a focal point for follow-on policy and training. However, the instances of the systems in question were covered by contingency actions and tests at other regional locations. At a follow-on meeting, documentation was provided that identified the locations of each system and to which enclave(s) the systems were appended.

3. The following section describes the Marine Corps response to IG recommendations:

a. Require system owners develop CP in accordance with the DITSCAP and the NIST SP 800-34 "Contingency Planning Guide for Information Technology Systems," when developing and testing DoD contingency plans.

(1) The Marine Corps concurs with this recommendation.

(2) The Marine Corps is currently developing CP templates based on the NIST publication. As part of the certification and accreditation documentation that is developed IAW the DITSCAP, a system CP is a required document. In addition, the template will be used to evaluate the MCEN enclave and site CP documentation. This does not preclude information systems from inheriting characteristics from both the enclave and sites to which the IS belongs.

b. Require that the DAA, the user representative, and the Certifying Authority approve contingency plans for information systems.

(1) The Marine Corps concurs with this recommendation.

(2) Currently, the MCEN DAA is responsible for accrediting the three MCEN enclaves. In accordance with the Marine Corps C&A process, the MCEN DAA is the sole accrediting authority for operational systems and is responsible for the final accreditation and acceptance of IA requirements for information systems used by the Marine Corps. As part of the C&A process, the Certifying Authority or his representative reviews the information systems documentation and provides an accreditation recommendation to the MCEN DAA for approval.

Subj: RESPONSE TO DEPARTMENT OF DEFENSE DRAFT REPORT DATED OCTOBER 2,2007; PROJECT NUMBER D2007-DOOOLB-0080.000

c. Require that CPs are tested under realistic conditions and in accordance with DoD Instruction 8500.2, "Information Assurance (IA) Implementation" and DoD Chief Information Officer Memorandum, "Department of Defense (DoD) Federal Information Security Management Act (FISMA) Guidance for Fiscal Year 2006, and document the results.

(1) The Marine Corps concurs with this recommendation.

(2) The Marine Corps has implemented a quarterly reporting schedule, where all Marine Corps IS are tested IAW DoD Instruction 8500.2. These results are documented and used to update Marine Corps DITPR data as required by FISMA.

d. Impose sanctions on system owners who do not prepare and test their systems' contingency plans or supply complete, accurate, and authoritative information in the DoD Information Technology Portfolio Repository.

(1) The Marine Corps concurs with this recommendation.

(2) Systems without complete security documentation, including contingency and disaster recovery plans, will not receive MCEN DAA accreditation and will be reported to the Marine Corps CIO for further action. This does not negate the ability of the information systems to be assigned to a MCEN enclave and site, inheriting characteristics of their CPs.

e. Implement automated controls, if applicable, on the Component system used to populate the DoD Information Technology Portfolio Repository to prevent blank data fields, duplicate .eporting of systems and system information, and reporting of different information for similar data fields.

(1) The Marine Corps concurs with this recommendation.

(2) The Marine Corps has implemented Telos Xacta IA Manager as the service certification and accreditation support tool. This tool will support reporting to DITPR-DON, which interfaces with DITPR.

f. Prepare a Component-level Plan of Action and Milestones, within 90 days of the issuance of the final report, noting that a significant number of the Component's mission-critical systems have security weaknesses related to contingency planning.

(1) The Marine Corps concurs with this recommendation.

(2) The Marine Corps is in the process of revalidating this information. The Marine Corps has fielded five two-person system security engineering teams, one team for each region world-wide, to oversee operational IA implementation and validation. Part of their charter includes support to local IA staffs in developing and feporting contingency after-action reporting, and to validate and remediate any security weakness found.

Subj: RESPONSE TO DEPARTMENT OF DEFENSE DRAFT REPORT DATED OCTOBER 2,2007; PROJECT NUMBER D2007-DOOOLB-0080.000

g. Require that owners of systems identified in this report as having security weaknesses in contingency planning develop a Plan of Action and Milestones within 90 days of the issuance of the final version of this report.

(1) The Marine Corps concurs with this recommendation.

(2) The Marine Corps will include this requirement in our annual FISMA message.

h. Review assertions made in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum, including whether the Component implemented automated controls, and certify to only the current state of the security status for the Components' information systems. Interview the information assurance professionals to verify that the information in the DoD Information Technology Portfolio Repository Chief Information Officer Memorandum is accurate.

(1) The Marine Corps concurs with this recommendation.

(2) The Marine Corps has implemented Telos Xacta IA Manager, an automated system security documentation and tracking tool, and included contingency reporting as a functionality.

i. Review any system designated as mission critical and Mission Assurance Category III to identify the rationale for the designation. Require that owners document the rationale in the System Security Authorization Agreement.

(1) The Marine Corps concurs with this recommendation.

(2) Marine Corps policy is that at a minimum all systems that are not public-access systems are designated as MAC III. The Marine Corps will work with system owners and program managers to complete this review and documentation to validate mission critical, mission essential, and mission support status.

G. J. ALLEN

Team Members

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

Robert F. Prinzbach II
Kimberley A. Caprio
Karen J. Goff
Barry Gay
Dawn M. Russell
Brenda M. Steib
Dharam V. Jain
Allison E. Tarmann

Inspector General
Department of Defense