Inspector General

United States Department of Defense

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
12 DEC 2006		**00-00-2006 to 00-00-2006**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **ODIG-AUD (ATTN: Audit Suggestions),Department of Defense Inspector General,400 Army Navy Drive (Room 801),Arlington,VA,22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**29**	

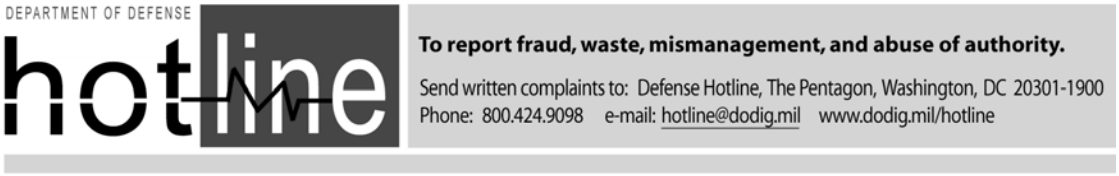
Additional Copies

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



Acronyms

C2G	Command and Control Guard
COOP	Continuity of Operations
DCTF	Defense Information Systems Agency Continuity of Operations and Test Facility
DISA	Defense Information Systems Agency
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
DRP	Disaster Recovery Plan
FEMA	Federal Emergency Management Agency
FPC	Federal Preparedness Circular
GAO	Government Accountability Office
GCSS	Global Combat Support System
IT	Information Technology
IG	Inspector General
JITC	Joint Interoperability Test Command
NIPRNET	Non-Secure Internet Protocol Router Network
OMB	Office of Management and Budget
PMO	Program Management Office
PM	Project Manager
SIPRNET	Secret Internet Protocol Router Network
SSAA	System Security Authorization Agreement
SWP	Severe Weather Plan

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

December 12, 2006

MEMORANDUM FOR DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY

SUBJECT: Report on the Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility (Report No. D-2007-031)

We are providing this report for your information and use. We considered management comments on a draft of this report when preparing the final report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. The Global Command Support System Program Management Office comments were partially responsive. We request additional comments on the recommendation by December 29, 2006. Comments should specifically address the date of the move of the Command and Control Guard suite and the date the new continuity of operations site for this suite will become operational.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to AudACM@dodig.mil. Copies of 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 (SIPERNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Jacqueline Wicecarver at (703) 604-9077 (DSN 664-9077) or Ms. Therese M. Kince at (703) 604-9060 (DSN 664-9060). See Appendix B for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Richard B. Jolliffe
Assistant Inspector General
Acquisition and Contract Management

Department of Defense Office of Inspector General

Report No. D-2007-031 **December 12, 2006**
(Project No. D2005-D000AS-0310.000)

The Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility

Executive Summary

Who Should Read This Report and Why? Military, civilians, and contractor personnel responsible for the implementation and oversight of DoD continuity of operations should read this report because it emphasizes the importance of continuity of operations planning for critical systems that may be disrupted during disasters.

Background. This audit report is the second in a planned series of audits on the effects of Hurricane Katrina on DoD information technology resources. The first report, DoD Inspector General Report No. D-2007-006, "Hurricane Katrina Disaster Recovery Efforts Related to Army Information Technology Resources," October 19, 2006, discussed the effects of Hurricane Katrina on Army information technology resources operated by the 321st Theater Materiel Management Center. The Defense Information Systems Agency Continuity of Operations and Test Facility (DCTF), located in Slidell, Louisiana, experienced communications disruptions as a result of Hurricane Katrina. DCTF provides information technology services that consist of integrated environments for product evaluation; technology; functional, developmental, performance, and information assurance testing; operational assessments and demonstrations; and knowledge management.

Federal policy requires all systems to have a contingency plan to ensure that service support continues through disruptions. In addition, DoD Directive 3020.26, "Defense Continuity Program," September 8, 2004, requires DoD Components to have a comprehensive and effective continuity program that ensures DoD Component mission-essential functions continue under all circumstances. The Directive also requires DoD Components to develop, coordinate, and maintain continuity plans; to update and reissue plans every 2 years; and to test and exercise continuity plans at least annually, or as otherwise directed.

Results. The DCTF personnel halted the testing mission to prepare for Hurricane Katrina. During the hurricane, personnel and the facility lost communications capabilities and the testing mission was not readily available for client use because no alternate means of testing was available. As a result, the DCTF testing mission was halted for 3 weeks following Hurricane Katrina (finding A). Also, the Command and Control Guard system, located at DCTF, could not continue real-time data processing following Hurricane Katrina. As a result, U.S. Army Europe, one of the primary DCTF Command and Control Guard users, lost real-time logistics data for 19 days (finding B). (See the Findings section of the report for the detailed recommendations). We identified internal control weaknesses at the DISA DCTF and the Global Combat Support System Program Management Office over the planning and protection of information technology resources.

Management Comments and Audit Response. The Commander, Joint Interoperability Test Command concurred with the recommendation that the Components that are gaining the DCTF testing mission update their continuity of operations plans so the plans meet Federal and DoD policy. The Commander, Joint Interoperability Test Command directed the Joint Interoperability Test Command components that gained the DISA Continuity of Operations and Test Facility testing mission to review and update their continuity of operations plans as appropriate. Updating the plans and changes were scheduled to be completed by December 1, 2006.

The Commander, Joint Interoperability Test Command concurred with the recommendation that DCTF update its System Security Authorization Agreement to include the termination of the continuity of operations mission and the continuation of the testing mission by January 2007. Specifically, the Commander stated that DCTF had submitted updates to the System Security Authorization Agreement to include the removal of the Secret Internet Protocol Router Network. Notice was also provided to the Chief Information Officer and the Strategic Planning and Information Directorate that the "Unclassified but Sensitive Internet Protocol Router Network" was scheduled to be turned off and removed on November 30, 2006. In response to the updates, the Defense Information Systems Agency's Strategic Planning and Information Directorate, Chief Information Officer, Information Assurance Branch, stated that no further updates to the Slidell System Security Authorization Agreement are required. However, the Information Assurance Branch will prepare amendments to the existing accreditation letter to reflect the removal of the Secret Internet Protocol Router Network and Cross Domain Solution and also the Unclassified but Sensitive Internet Protocol Router Network after its scheduled termination on November 30, 2006.

The Global Combat Support System Program Management Office concurred with the recommendation to complete the Contingency Management Plan for the Command and Control Guard system to comply with Federal policy. The Global Combat Support System Program Management Office stated that the Secret In-Transit Visibility system has transitioned to the primary Command and Control Guard system administered by Systems Management Center in Montgomery, Alabama. In addition, the Program Management Office completed, the Command and Control Guard system suite move from the DCTF in Slidell, Louisiana, to the Defense Enterprise Computing Center-Pacific, which will be the continuity of operations site for the Command and Control Guard system. The Program Management Office also plans to develop a Contingency Management Plan for the Command and Control Guard system to comply with the Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," by December 1, 2006.

We request that the Global Combat Support System Program Management Office provide comments to the final report by December 29, 2006. Specifically, the Program Management Office should provide the completion date of the Command and Control Guard suite move to the Defense Enterprise Computing Center-Pacific and the date the new continuity of operations site will become operational.

Table of Contents

Executive Summary i

Background 1

Objective 3

Review of Internal Controls 3

Findings

A. Defense Information Systems Agency Continuity of Operations and Test Facility Continuity of Operations 4
B. Command and Control Guard Continuity of Operations Plan 11

Appendixes

A. Scope and Methodology 15
Prior Coverage 16
B. Report Distribution 17

Management Comments

Joint Interoperability Test Command 19
Global Combat Support System Program Management Office 21

Background

This audit is the second in a series of planned audits on the effects of Hurricane Katrina on DoD information technology (IT) resources. The first report, DoD Inspector General (IG) Report No. D-2007-006, "Hurricane Katrina Disaster Recovery Efforts Related to Army Information Technology Resources," October 19, 2006, discussed the effects of Hurricane Katrina on Army IT resources operated by the 321st Theatre Materiel Management Center. For this audit, we focused on the effects of Hurricane Katrina on IT resources at the Defense Information Systems Agency (DISA) Continuity of Operations and Test Facility (DCTF) located in Slidell, Louisiana.

DISA Mission. The designated core missions of DISA are communications, joint command and control, defensive information operations, combat support computing, and joint interoperability support.

The majority of the DoD command and control and combat support information uses the joint networks provided by DISA, collectively referred to as the Defense Information Systems Network. The Defense Information Systems Network provides interoperable, secure Internet Protocol data communications services. Two specific subsystems on the Defense Information Systems Network include the Secret Internet Protocol Router Network (SIPRNET) and the Non-Secure Internet Protocol Router Network (NIPRNET).[1] The SIPRNET is a system of interconnected computer networks used by DoD to transmit classified information in a secure environment. The NIPRNET is used to exchange unclassified but sensitive information between internal users as well as providing users access to the Internet. At the time of Hurricane Katrina, DCTF housed and provided manpower support to the Command and Control Guard (C2G) system, a system that transfers logistics data between the NIPRNET and the SIPRNET.

DCTF. The mission at the DCTF has changed several times over the past 10 years. In 1995, DCTF was designated as a Continuity of Operations (COOP) center for the DISA Enterprise Computing Centers. In 1996, developmental test and security evaluation services were added to the DCTF mission. In October 2004, the COOP mission was terminated and DCTF continued with its testing mission. DCTF provides IT services that consist of integrated environments for product evaluation; technology; functional, developmental, performance, and information assurance testing; operational assessments and demonstrations; and knowledge management. On October 1, 2005, DCTF was placed under the direction of the Joint Interoperability Test Command (JITC) in Fort Huachuca, Arizona. JITC is an independent field operational test and evaluation command for DISA, Command, Control, Communications, Computers, and Intelligence and identifies interoperability deficiencies through testing and evaluation.

The DCTF has been identified for closure in the DoD Base Closure and Realignment Commission list. According to JITC personnel, DISA plans to close DCTF in January 2007. During the audit, the DCTF testing mission moved to

[1] NIPRNET is also referred as the Unclassified but Sensitive Internet Protocol Router Network.

JITC locations at Fort Huachuca, Arizona; Indian Head, Maryland; and Falls Church, Virginia.

Criteria

All DoD organizations are required to comply with the following policies when they implement their disaster recovery controls and plans.

Federal Emergency Management Agency Federal Preparedness Circular 65. The Federal Emergency Management Agency (FEMA) Federal Preparedness Circular (FPC) 65, "Federal Executive Branch Continuity of Operations (COOP)," July 26, 1999, provides guidance on COOP planning procedures and elements of a COOP plan. The guidance is applicable to all Federal Executive Branch departments, agencies, and independent organizations. According to FPC 65, a COOP plan should ensure the continuous performance of an agency's essential functions/operations during an emergency, ensure the protection of essential facilities and equipments, reduce or mitigate disruptions to operations, reduce loss of life and minimize damage, achieve a timely and orderly recovery from an emergency, and resume full service to customers.

Office of Management and Budget Circular No. A-130. Office of Management and Budget (OMB) Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000, (Appendix III) requires systems to have a contingency plan to ensure service support continues through disruptions. In addition, Appendix III provides security requirements for major applications, which require special security measures due to the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to the information. Appendix III requires that major applications have a periodically tested contingency plan that will ensure the agency function supported by the application will continue if automated support fails. It also states that agency plans should ensure that there is an ability to recover and provide service sufficient to meet the system users' minimal needs. Further, Appendix III states that manual procedures are generally not a viable back-up option.

DoD Directive 3020.26. DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004, requires a comprehensive and effective continuity program that ensures DoD Component mission-essential functions continue under all circumstances and threats. Also, the performance of mission-essential functions in a continuity threat or event shall be the basis for continuity planning, preparation, and execution. This directive orders the heads of the DoD Components to develop, coordinate, and maintain continuity plans and to update and reissue plans every 2 years. Finally, the heads of the DoD Components should test and exercise continuity plans at least annually, or otherwise as directed.

DoD Instruction 5200.40. DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, provides a single approach to activities leading to certification and accreditation within DoD. The objective of the DITSCAP is to establish a DoD standard certification and accreditation approach, which protects

and secures the entities comprising the Defense Information Infrastructure. One of the basic documents produced under the DITSCAP is the System Security Authorization Agreement (SSAA). The SSAA describes the system missions, target environment, target architecture, security requirements, and applicable data access policies. It also describes the applicable set of planning and certification actions, resources, and documentation required supporting certification and accreditation. As such, it is a living document that represents the formal agreement among the Designated Approving Authority, the Certification Authority, the user representative, and the program manager.

Objective

The overall audit objective was to determine the effects of Hurricane Katrina on DoD IT resources in affected areas. Specifically, we reviewed IT resources managed by DCTF that were affected by Hurricane Katrina. See Appendix A for a discussion of the scope and methodology and prior audit coverage related to the objective.

Review of Internal Controls

We identified internal control weaknesses for DCTF as defined by DoD Instruction 5010.40, "Managers' Internal Control (MIC) Program Procedures," January 4, 2006. DoD 5010.40 states that internal controls are the organization, policies, and procedures that help program and financial managers to achieve results and safeguard the integrity of their programs. We identified internal control weaknesses at the DISA DCTF and Global Combat Support System Program Management Office. DCTF management did not have procedures in place to ensure that the Severe Weather Plan (SWP) and SSAA complied with Federal and DoD policy. When the JITC components that are gaining the DCTF testing mission update their continuity of operations plans to meet the requirements identified in Federal and DoD policy, internal controls over the testing mission should improve. The Global Combat Support System, Program Management Office did not have a COOP plan to adequately protect and safeguard the C2G system at the DISA DCTF. When the Global Combat Support System Program Manager completes the Contingency Management Plan for the C2G it should improve internal controls over the C2G.

A. Defense Information Systems Agency Continuity of Operations and Test Facility Continuity of Operations

The DCTF personnel halted the testing mission to prepare for Hurricane Katrina. During the hurricane, personnel and the facility lost communications capabilities and the testing mission was not readily available for client use because no alternate means of testing was available. This occurred because DCTF and DISA COOP officials did not validate and test that the SWP and the SSAA complied with Federal and DoD policy. For example, neither the SWP nor the SSAA included specific procedures to reduce disruptions to the DCTF testing mission. As a result, DCTF was not able to provide the testing mission for 3 weeks.

Testing Mission

The DCTF personnel halted the testing mission to prepare for Hurricane Katrina. The following provides the approximate timeline of events performed by DCTF and JITC personnel.

- August 26, 2005: DCTF officials implemented the SWP.
- August 27, 2005: DCTF officials released non-essential personnel.
- August 28, 2005: DCTF officials recalled emergency essential personnel and took in Slidell first responders, equipment, and DISA families.
- August 29, 2005: Hurricane Katrina made landfall, causing communications outages; DCTF employees could not communicate with DISA Headquarters. The facility sustained minor damage and a generator provided portions of the facility with power.
- September 5, 2005: JITC representatives provided DCTF with a communications package, although not part of either the SWP or SSAA. The communications package included satellite phones, access to the NIPRNET and SIPRNET, and video teleconferencing.
- September 8, 2005: DCTF officials accounted for all employees.
- September 19, 2005: DCTF officials determined enough DCTF personnel returned to resume the testing mission.

Disaster Planning

The testing mission was negatively impacted because the DCTF SWP and SSAA did not comply with Federal and DoD policy. DCTF officials were responsible for updating both the SWP and the SSAA.

COOP Criteria. Federal and DoD policies state that every comprehensive COOP plan should have the following key criteria elements that:

- provide for the continuous performance of an agency's essential functions/operations during an emergency;
- reduce or mitigate disruptions to operations;
- ensure the protection of essential facilities and equipments;
- develop, coordinate, and maintain continuity plans, and update and reissue plans every 2 years;
- address communication support to continuity operations; and
- identify relocation sites or platforms for Component use during continuity threats or events.

DCTF COOP. DCTF Instruction 200-50-5, "Severe Weather Plan [SWP]," May 19, 2005, and the DCTF SSAA did not comply with Federal and DoD policy to ensure continuity of operations. The DCTF officials considered the DCTF SWP to be their COOP for responding to severe weather conditions. The SWP outlined steps to be taken by DCTF before, during, and after severe weather conditions.

The DCTF SSAA documented the DCTF certification and accreditation process to obtain site re-accreditation. The DCTF SSAA contains security documentation to include the DCTF Disaster Recovery Plan (DRP), September 2003, and the Vulnerability Assessment and Risk Analysis, April 13, 2003.

In the following table we evaluated the SWP and DRP to determine whether the plans outline procedures regarding these six key criteria elements of a COOP plan as required by FPC 65 and DoD 3020.26. The following table uses green, yellow, and red to indicate the effectiveness of the plans in these criteria elements.

DCTF Continuity of Operations Plans and Analysis of Key Criteria Elements		
Key Criteria Elements	**Severe Weather Plan**	**System Security Authorization Agreement (Disaster Recovery Plan)**
Mission-Essential Functions	**Red**	**Red**
Reduce or Mitigate Disruption to Operations	**Red**	**Yellow**
Protection of Essential Facilities and Equipment	**Yellow**	**Red**
Develop, Coordinate, and Maintain Continuity Plans	**Green**	**Yellow**
Communication Support	**Red**	**Yellow**
Relocation of Sites or Platforms	**Red**	**Green**
Green=Plan includes information that does not need to be updated. Yellow=Plan includes outdated or incomplete information. Red=Plan does not include information.		

Mission-Essential Functions. Mission-essential functions are those tasks that must be performed under all circumstances to achieve missions or responsibilities in a continuity threat or event. Failure to perform or sustain these functions would significantly impact the ability of DoD to provide vital services, or exercise authority, direction, and control. According to the DCTF SSAA, the DCTF fills extremely critical roles and has time-sensitive missions that cannot be easily performed by other organizations. The DCTF SSAA also maintains that the criticality of the DCTF COOP and test missions are very high. Specifically, the DCTF SSAA states that its mission and functions provide flexible environments to perform system integration, security, and stress testing of command and control software systems.

Clients relied on DCTF to continue its testing mission for their programs. For example, the eBusiness[2] service level agreement deliverables included planning

[2]The eBusiness Program Portfolio is composed of eight programs that facilitate business transactions within the Federal Government. There are two types of programs, Federal-wide and DoD.

for, conducting, and reporting against the performance testing of systems. As a result of the testing mission downtime, the eBusiness Program Portfolio Program Manager decided to relocate the system testing due to his concern that the downtime would hamper the ability of the program to meet an important testing milestone.

Neither the SWP nor the DRP were updated after October 2004 to reflect the change in the DCTF mission. While the SWP stated that DCTF will "maintain comprehensive and aggressive plans to protect its mission capability," the SWP did not outline the DCTF mission-essential functions.

The DRP provided continuity procedures for the DCTF COOP mission, which was terminated in October 2004, and for the DCTF test mission; however, the DRP did not define the mission-essential functions for either mission.

Reduce or Mitigate Disruption to Operations. Disruption to operations procedures should be addressed in a COOP plan to achieve a timely and orderly recovery from an emergency and resume full service to customers. While the DRP did include critical recovery time frames for testing, COOP, communications, and payroll, neither the SWP nor the DRP provided specific procedures to reduce disruptions to the DCTF testing mission.

Protection of Essential Facilities and Equipment. Federal and DoD policy require COOP plans to outline procedures to ensure the protection of essential facilities and equipment; neither the SWP nor the DRP fully satisfied the policy requirements for this element. The SWP provided a list of actions to be taken before, during, and after the threat of severe weather to ensure the protection of the facility; however, the plan did not address the protection of the test equipment. In addition, the DRP did not address either the protection of the facility or the protection of test equipment.

Develop, Coordinate, and Maintain Continuity Plans. According to DoD Directive 3020.26, COOP plans should be developed, coordinated, and maintained by DoD Component Heads and updated and reissued every 2 years or as changes occur. The SWP is updated and reissued each year by the Chief of DCTF. DCTF officials updated the SWP on April 12, 2006. However, DCTF officials did not update the DRP within the 2-year time frame. During the time DCTF was not operational, following Hurricane Katrina, the DRP became outdated.

DCTF officials were not prepared for severe weather conditions of Hurricane Katrina's magnitude, which was reflected in the development of the SSAA. For example, Appendix G of the SSAA, "Vulnerability Assessment and Risk Analysis," April 13, 2003, did not include the threat of a disruption to communications services due to severe emergency conditions such as hurricanes or tornadoes.

Communication Support. Available and redundant critical communications should be addressed in the COOP plan to support connectivity to internal organizations, other agencies, critical customers, and the public. Although DISA had redundant communications, the DCTF SWP did not address this key element.

In addition, the DRP did not contain procedures for available voice and data communications in the event the commercial communications infrastructure was damaged in the surrounding area.

Relocation of Sites or Platforms. Alternate operating facilities or platforms should be designated for use during continuity threats or events. In addition, personnel should be prepared for the unannounced relocation of essential functions to these facilities. The SWP did not identify a disaster recovery contingency site for the DCTF testing mission. The DRP identified the disaster recovery contingency site for the testing mission as DISA headquarters but stated that if DISA headquarters test assets were not available, the testing function would be deferred. The testing mission was not transferred to DISA headquarters following Hurricane Katrina. As a result, the eBusiness Program Portfolio Program Manager decided to relocate the system testing due to his concern that the downtime would hamper the ability of the program to meet an important testing milestone.

Both the SWP and DRP did include names and titles of essential employees who were to stay at the facility in case of an emergency. In addition, the SWP stated that employees are issued cards with key points of contact and phone numbers that may be called before and after severe weather conditions or after a disaster. However, a specific designated area for non-emergency essential employees to report to during an emergency was not included in either the SWP or DRP. As a result, not all DCTF employees and their families were accounted for until approximately 10 days after Hurricane Katrina.

Planning Oversight

The testing mission was negatively impacted because DISA COOP officials did not provide sufficient oversight to ensure the DCTF continuity of operations and security documents complied with Federal and DoD policy.

SWP. Personnel at the DISA Concepts and COOP Branch, under the DISA Plans, Concepts, and Integration Division, agreed that the SWP did not meet Federal or DoD COOP policy. According to personnel in the DISA Concepts and COOP Branch, they asked DCTF for COOP information related to mission-essential functions in 2002. However, the DISA COOP Branch concentrated its request for mission-essential function COOP data to the National Capital Region, and did not require DISA field sites to respond. DCTF did not respond and there was no follow-up until our audit. During our audit, the DISA COOP Branch sent another data call requesting information regarding mission-essential functions to all field sites. JITC personnel stated that DISA Test and Evaluations Directorate determined DCTF did not have any mission-essential functions; therefore, DCTF did not provide information to the DISA COOP Branch.

SSAA. The DCTF Information Assurance Officer did not provide sufficient oversight to ensure the SSAA complied with DoD policy. DoD Instruction 5200.40 requires the SSAA to be updated whenever necessary to reflect the current operating system mission. According to the Defense Switched

Network Site SSAA Template, March 1, 2004, the Information Assurance Officer who is appointed at the organizational level will be responsible for developing the certification and accreditation documentation for his/her organization. According to the DCTF SSAA in effect at the time of Hurricane Katrina, the criticality of the affected COOP mission was very high; however, DCTF had not been responsible for the COOP mission since October 2004. The Information Assurance Officer had not revised the DCTF SSAA to reflect the mission change to the testing mission.

On April 24, 2006, the DISA Chief Information Officer granted an Interim Authority to Operate dated to expire in January 2007. The Interim Authority to Operate requires DCTF to continue to revise the SSAA. Therefore, DCTF should update the SSAA in accordance with the Interim Authority to Operate to include all changes that have occurred since the October 23, 2000, site accreditation.

Management Actions

DCTF officials updated the SWP on April 12, 2006. The April 2006 version included the addition of the Emergency Planning Information Sheet enclosure, which included a form that DCTF employees must complete and return to their Branch Chief. The new form should allow for better personnel accountability in the event of a disaster. In addition, after Hurricane Katrina, DCTF developed a lessons learned document on how the facility could better handle a hurricane of this magnitude. However, the updated SWP was not revised to include the contingency actions lessons learned based on the magnitude of Hurricane Katrina.

Following Hurricane Katrina, DISA officials initiated a DISA-wide review and assessment of mission-essential functions to help organizations identify tools needed to accomplish their mission.

Recommendations and Management Comments

A.1. We recommend that the Commander, Joint Interoperability Test Command require Joint Interoperability Test Command Components that are gaining the Defense Continuity of Operations and Test Facility testing mission to update their continuity of operations plans so the plans meet Federal and DoD Continuity of Operations policy and for these Components to review their Continuity of Operations plans on an annual basis and update whenever major changes occur.

Management Comments. The Commander, Joint Interoperability Test Command concurred. The Commander, Joint Interoperability Test Command directed the Joint Interoperability Test Command components that gained the DISA Continuity of Operations and Test Facility testing mission to review and update their continuity of operations plans as appropriate. Updates to the plans and changes were schedule to be completed by December 1, 2006.

A.2. We recommend that the Commander, Joint Interoperability Test Command require the Defense Information Systems Agency Continuity of Operations and Test Facility to update its System Security Authorization Agreement to include the termination of the continuity of operations mission and the continuation of the testing mission by January 2007.

Management Comments. The Commander, Joint Interoperability Test Command concurred. Specifically, the Commander stated that DCTF had submitted updates to the System Security Authorization Agreement to include the removal of the Secret Internet Protocol Router Network. Notice was also provided to the Chief Information Officer and the Strategic Planning and Information Directorate that the "Unclassified but Sensitive Internet Protocol Router Network" was scheduled to be turned off and removed on November 30, 2006. In response to the updates the Defense Information Systems Agency's Strategic Planning and Information Directorate, Chief Information Officer, Information Assurance Branch, stated that no further updates to the Slidell System Security Authorization Agreement are required. However, the Information Assurance Branch will prepare amendments to the existing accreditation letter (or a new decision) to reflect the removal of the Secret Internet Protocol Router Network and Cross Domain Solution and also the Unclassified but Sensitive Internet Protocol Router Network after it is terminated on November 30, 2006.

B. Command and Control Guard Continuity of Operations Plan

The Command and Control Guard (C2G) system, located at DCTF, could not continue real-time data processing following Hurricane Katrina. This occurred because the DISA Global Combat Support System (GCSS) Program Management Office, owner of the C2G, did not have a formal COOP plan for the C2G system. As a result, U.S. Army Europe, one of the primary DCTF C2G users, lost real-time Radio Frequency-In-Transit Visibility system logistics data for 19 days.

Lost Connectivity

The C2G system, the only operational system located at DCTF, could not continue real-time data processing following Hurricane Katrina. The C2G system lost connectivity because the commercial communications infrastructure in Slidell, Louisiana, was severely damaged. The C2G system is used to automatically transfer logistics information from the NIPRNET to the SIPRNET to ensure the SIPRNET is updated on a real-time basis. According to the DISA Requirements Memorandum, April 20, 2005, "Cross Domain Connection to support Global Combat Support Systems (GCSS) Command and Control Guard (C2G) Operations in SMC Montgomery," (the DISA Requirements Memorandum) the C2G supports warfighter access to critical logistics data. At the time of Hurricane Katrina, the primary users of the DCTF C2G were U.S. Army Europe and the Defense Logistics Agency.

Prior to Hurricane Katrina, DCTF operated 8 hours a day, 5 days a week, which was insufficient for the C2G user community. As a result, DCTF officials began transferring the primary users of the C2G system to the System Management Center in Montgomery, Alabama, which operates 24 hours a day, 7 days a week. The Defense Logistics Agency users were successfully transferred to the System Management Center approximately one day after Hurricane Katrina; however, the System Management Center had not been configured to accommodate the U.S. Army Europe users at the time of the hurricane. After the Defense Logistics Agency users were transferred to the System Management Center, DCTF became the back-up site for the C2G that supports the Defense Logistics Agency. However, DCTF remained the primary site for the U.S. Army Europe users.

COOP Plan

The DISA GCSS Program Management Office, owner of the C2G, had not completed a COOP plan for the C2G system. Federal policy requires systems to have a contingency plan to ensure service support continues through disruptions. GCSS personnel provided a draft C2G Contingency Management Plan. This plan was not implemented during Hurricane Katrina and still has not been finalized and approved.

Federal System Security Requirements. OMB Circular No. A-130, Appendix III requires systems to have a contingency plan to ensure service support continues through disruptions. Based on the DISA Requirements Memorandum, the logistics information transferred through the C2G is critical and supports the warfighter.

Appendix III requires that major applications have a periodically tested contingency plan that will ensure the agency function supported by the application will continue if automated support fails. It also states that agency plans should ensure that there is an ability to recover and provide service sufficient to meet the system users' minimal needs. Further, Appendix III states that manual procedures are generally not a viable back-up option.

DISA GCSS did not have procedures to ensure the C2G system maintained connectivity in the event the primary site, DCTF, was unavailable. Because the C2G did not have an accessible contingency site, a contractor working for U.S. Army Europe manually transferred the logistics data from the NIPRNET to the SIPRNET approximately two times per day during the 19 days of the system downtime. The DISA Requirements Memorandum states that the logistics information transferred from NIPRNET to SIPRNET is time-sensitive and manually transferring the data from one source to another is not acceptable because the data would not be updated on a real-time basis. Therefore, based on OMB Circular No. A-130 and the DISA Requirements Memorandum, the manual transfer did not effectively support the C2G mission and the downtime impacted the quality of the logistics data because U.S. Army Europe users were not receiving information on a real-time basis. The GCSS officials should develop a COOP plan to ensure the C2G maintains network connectivity through a disaster situation.

Draft Contingency Plan. An official from the GCSS Program Management Office developed a C2G Contingency Management Plan that provided the overall strategy for implementing and operating the C2G. The plan was not completed or signed by a DISA official and therefore, was not implemented during Hurricane Katrina. The Contingency Management Plan was incomplete in the following areas:

- specific requirements and locations for continuous operations had not been determined;
- maximum lost data intervals, used to determine the frequency of data backup, was not provided;
- maximum downtime, used to determine contingency management strategies for preventing service-level interruptions and for restoring limited production, was not provided; and
- planned actions in the event the primary C2G site, the System Management Center in Montgomery, Alabama, and the back-up C2G site in Slidell, Louisiana, were unavailable.

Impact of the C2G Downtime

As a result of the C2G downtime, U.S. Army Europe lost real-time logistics data to support the warfighter for 19 days. Specifically, the system used by U.S. Army Europe, the Radio Frequency-In-Transit Visibility system, to obtain real-time logistics data was disrupted due to the C2G downtime. The Radio Frequency-In-Transit Visibility system supports warfighter operations and uses the logistics information transferred by the C2G system. Therefore, the lack of a contingency plan resulted in the warfighter not receiving real-time logistics information from the Radio Frequency-In-Transit Visibility system. Unless DISA GCSS completes the contingency plan for the C2G and ensures the plan includes the elements required by OMB Circular A-130, Appendix III, the probability that the C2G will be unable to effectively support the warfighter during another communication disruption is significant.

Management Planning

In 2006, DISA successfully transferred the U.S. Army Europe C2G users to the System Management Center in Montgomery, Alabama. Consequently, DCTF also became the back-up site for the U.S. Army Europe C2G users. Due to DCTF being identified on the 2005 Base Realignment and Closure list, the personnel administering the back-up C2G system at DCTF accepted other employment in July 2006. Therefore, DCTF lacked personnel available to administer the contingency function of the C2G system. According to DISA personnel, DISA configured the Defense Enterprise Computing Center at the DISA Pacific Field Command at Pearl Harbor, Hawaii, to be the back-up site for both primary users of the C2G system as of August 7, 2006.

Recommendations, Management Comments, and Audit Response

We recommend the Program Manager, Defense Information Systems Agency Global Combat Support System complete the Contingency Management Plan for the Command and Control Guard system to comply with the Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000.

Management Comments. The Global Combat Support System Program Management Office concurred, stating that the Secret In-Transit Visibility system has transitioned to the primary C2G administered by the Systems Management Center in Montgomery, Alabama. In addition, the Program Management Office completed the C2G suite move from the DCTF in Slidell, Louisiana, to the Defense Enterprise Computing Center-Pacific, which will be the COOP site for the C2G. The Program Management Office also planned to develop a Contingency Management Plan for the Command and Control Guard system to comply with the Office of Management and Budget Circular No. A-130,

Appendix III, “Security of Federal Automated Information Resources by December 1, 2006.

Audit Response. Although the Global Combat Support System Program Management Office concurred with the recommendation, the comments were partially responsive in that a completion date that the Command and Control Guard suite was moved to the Defense Enterprise Computing Center-Pacific and a date when the new continuity of operations site will become operational was not provided. Therefore, we request that the Global Combat Support System Program Management Office provide these completion dates and planned actions to the final report by December 29, 2006.

Appendix A. Scope and Methodology

We performed this audit from October 2005 through September 2006 in accordance with generally accepted government auditing standards. This audit is the second in a planned series of audits that will be conducted to determine the effects of Hurricane Katrina on DoD IT resources. The scope of this audit was limited to determining the effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility located in Slidell, Louisiana.

We conducted field work at DISA offices located in the National Capital Region and at the DCTF in Slidell, Louisiana; and the Program Executive Office for Enterprise Information Systems in Fort Belvoir, Virginia. Additionally, we reviewed and analyzed continuity of operation procedures and disaster plans to determine what recovery actions were performed before, during, and after Hurricane Katrina, and the effect Hurricane Katrina had on DCTF IT resources. Additionally, we talked to the Army Program Executive Office for Enterprise Information Systems and the Defense Logistics Agency Program Management Office for Asset Visibility to discuss the effect of the downtime of the C2G system and the effect of the downtime on U.S. Army Europe and the Defense Logistics Agency.

We obtained information for the audit through meetings, e-mails, and briefings with the personnel stated above. We reviewed and analyzed laws, policies, guidance, and documentation dated from December 30, 1997, through April 12, 2006. Specifically, we reviewed and compared:

- FEMA FPC 65, "Federal Executive Branch Continuity of Operations (COOP)," July 26, 1999;
- OMB Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000;
- DoD Directive 3020.26, "Defense Continuity Program (DCP)," September 8, 2004;
- DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997;
- DCTF Severe Weather Plan, May 19, 2005; and
- DCTF System Security Authorization Agreement, undated, which included:
    - DCTF Vulnerability Assessment and Risk Analysis, April 13, 2003;

- "DISA Continuity of Operations and Test Facility (DCTF) Slidell, Louisiana, Disaster Recovery Plan (DRP)," September 2003; and

- DCTF Severe Weather Plan, April 12, 2006.

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

Government Accountability Office High-Risk Area. The Government Accountability Office (GAO) 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, GAO has issued one report and the DoD IG issued one report on continuity planning and emergency recovery efforts and the effects of Hurricane Katrina. Unrestricted GAO reports can be accessed over the Internet at http://www.gao.gov. Unrestricted DoD IG reports can be accessed at http://www.dodig.mil/audit/reports.

GAO

GAO Report GAO-04-160, "Continuity of Operations: Improved Planning Needed to Ensure Delivery of Essential Government Services," February 27, 2004

DoD IG

DoD IG Report No. D-2007-006, "Hurricane Katrina Disaster Recovery Efforts Related to Army Information Technology Resources," October 19, 2006

Appendix B. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
    Director, Acquisition Resources and Analysis
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
Director, Program Analysis and Evaluation
Under Secretary of Defense for Personal and Readiness
Assistant Secretary of Defense for Network and Information Integration/DoD Chief Information Officer

Department of the Army

Assistant Secretary of the Army (Financial Management and Comptroller)
Auditor General, Department of the Army
Program Executive Office Enterprise Information Systems

Department of the Navy

Naval Inspector General
Auditor General, Department of the Navy

Department of the Air Force

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

Combatant Commands

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

Other Defense Organizations

Director, Defense Information Systems Agency
    Director, Test and Evaluation Directorate
        Chief, Defense Information Systems Agency Continuity of Operations and Test Facility
Director, Defense Logistics Agency
Director, National Guard Bureau
Directors of the DoD Field Activities

Non-Defense Federal Organization

Office of Management and Budget
Office of Inspector General, Department of Homeland Security

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 Government Reform
House Subcommittee on Government Management, Finance, and Accountability, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform

Joint Interoperability Test Command Comments

DEFENSE INFORMATION SYSTEMS AGENCY
JOINT INTEROPERABILITY TEST COMMAND
P.O. BOX 12798
FORT HUACHUCA, ARIZONA 85670-2798

NOV 07 2006

IN REPLY REFER TO: Commander (JT)

MEMORANDUM FOR DEPARTMENT OF DEFENSE INSPECTOR GENERAL

THROUGH: DEFENSE INFORMATION SYSTEMS AGENCY INSPECTOR GENERAL

SUBJECT: DoD Report on the Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility (Project NO. D2005-DOOOAS-03 10.000)

1. The Defense Information Systems Agency has reviewed the subject draft report dated 12 October 2006 and provides their comments at the enclosure. We thank the DoD Inspector General Audit Team for the opportunity to participate in this audit and trust that we provided information that is deemed useful in completing this task.

2. We look forward to continuing to work with you and your staff in the future. My action officer is Mr. Michael Lynch, Chief, Contracts and Agreements Branch, (520) 538-5006. Please do not hesitate to call Mr. Lynch should you wish to discuss our response.

1 Enclosure:
DISA Response

DEBRA A. DEXTER
Colonel, USAF
Commander

ODIG DRAFT REPORT
Project Number D2005-D000AS-0310.000

The Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility

DEFENSE INFORMATION SYSTEMS AGENCY COMMENT TO FINDINGS:

RECOMMENDATION A.1. We recommend that the Commander, Joint Interoperability Test Command require Joint Interoperability Test Command Components that are gaining the Defense Continuity of Operations and Test Facility (DCTF) testing mission to update their continuity of operations plans so the plans meet Federal and DoD Continuity of Operations policy and for these Components to review their Continuity of Operations plans on an annual basis and update whenever major changes occur.

JITC Response. Concur. The Commander, Joint Interoperability Test Command has directed the Joint Interoperability Test Command Components that gained the DCTF testing missions to review and update their continuity of operations plans as appropriate. Actions to update the plans are ongoing and the changes to include the DCTF test missions will be completed by 1 December 2006. JITC Fort Huachuca POC is Mr. Ron Morales and JITC Indian Head POC is Mr. George Johnson.

RECOMMENDATION A.2. We recommend that the Commander, Joint Interoperability Test Command require the DCTF to update its System Security Authorization Agreement to include the termination of the continuity of operations mission and the continuation of the testing mission by January 2007.

JITC Response. Concur. The Defense Information Systems Agency DCTF has submitted updates to the System Security Authorization Agreement. Most recently an update was provided to reflect the removal of the Secret Internet Protocol Router Network (SIPRNet) at which time notice was also provided to the Chief Information Officer (CIO) and the Strategic Planning and Information Directorate (SPI) that the Unclassified but Sensitive Internet Protocol Router Network (NIPRNet) would be turned off and removed on 30 November 2006. In response, the DISA SPI/CIO Information Assurance Branch stated that no further updates to the Slidell SSAA are required. The Information Assurance Branch also took internal taskings to prepare an amendment to the existing accreditation letter (or a new decision) to remove the SIPRNet and Cross Domain Solution and to do another amendment when the NIPRNet is terminated on 30 November 2006. JITC POC is Mr. Garrett Wasson.

Enclosure 1

Global Combat Support System Program Management Office Comments

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

IN REPLY REFER TO

Program Management Office, Global Combat Support System (CC2) NOV 8 2006

TO: DOD Inspector General

THRU: Director, C2 Programs

SUBJECT: The Effects of Hurricane Katrina on the Defense Information Systems Agency Continuity of Operations and Test Facility, Project No. D-2005-D000AS-0310.000 dated October 12, 2006

1. The Program Management Office, Global Combat Support System (PMO, GCSS) concurs with the findings by the DOD IG, as documented in subject project, paragraph B. The GCSS PMO has since transitioned the S-ITV to the primary C2G which is administered by Systems Management Center-Montgomery, AL. The PMO completed the move of the C2G suite from the DCTS in Slidell, Louisiana to the Defense Enterprise Computing Center-Pacific (DECC-PAC), which will be the COOP site for the C2G.

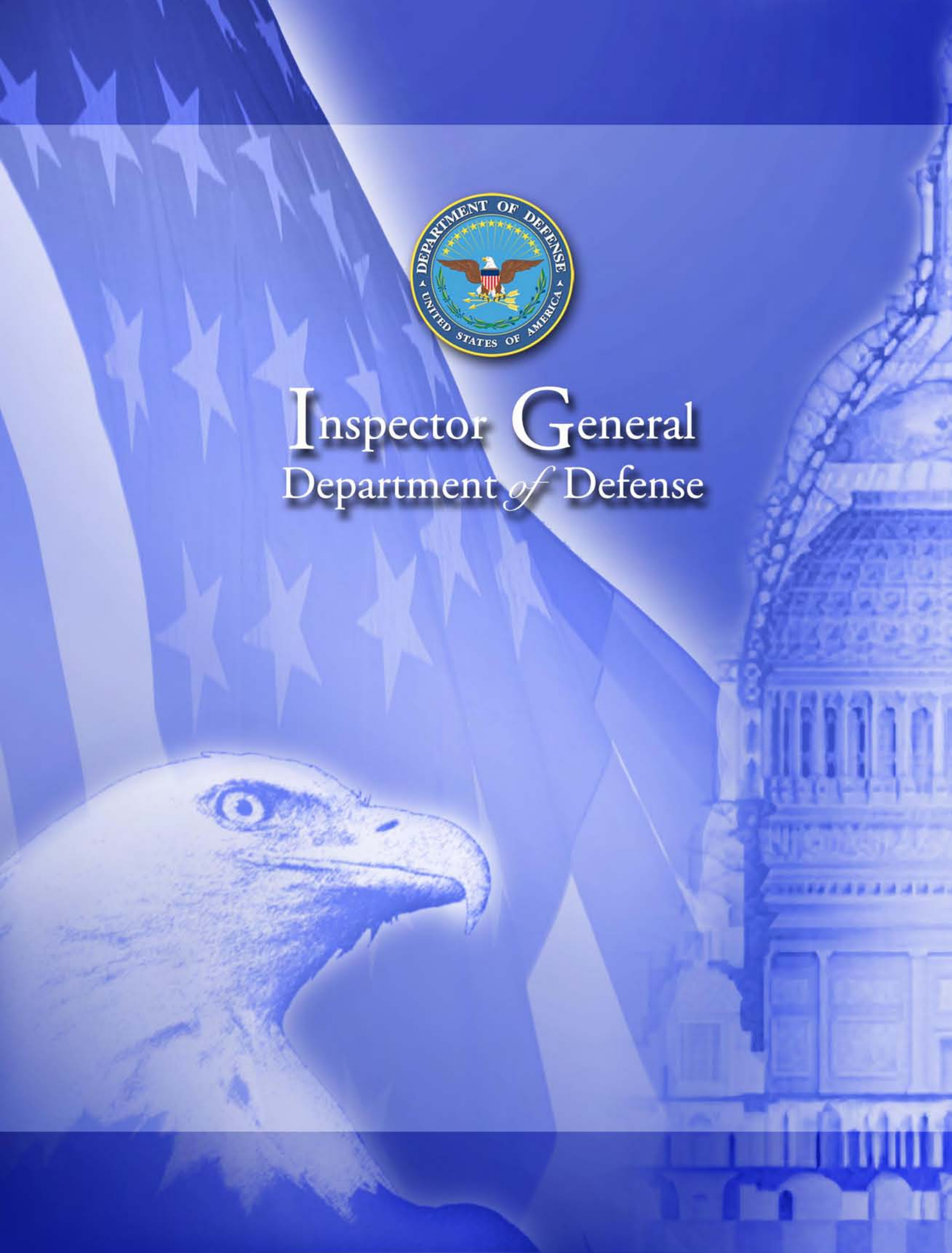
2. The GCSS PMO will develop a Contingency Management Plan for the C2G to comply with the Office of Management and Budget Circular No. A-130, Appendix III, "Security of Federal Automated Information Resources," November 28, 2000. This Plan will be completed by 1 December 2006.

PAULA FRIEDMAN
Program Manager
Global Combat Support System

Team Members

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

Richard B. Jolliffe
Bruce A. Burton
Jacqueline L. Wicecarver
Therese M. Kince-Campbell
Kelly B. Lesly
Susan R. Ryan
Richard A. Pinnock
Susan H. Bachle
Pedro J. Calderón
Adrianne R. Voshell
Meredith H. Johnson



Inspector General
Department of Defense