Audit Report

SECURITY CONTROLS OVER CONTRACTOR SUPPORT
FOR YEAR 2000 RENOVATION

Report No. D-2001-016 December 12, 2000

Office of the Inspector General
Department of Defense

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 12Dec2000	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Security Controls Over Contractor Support for Year 2000 Renovation	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) OAIG-AUD (ATTN: AFTS Audit Suggestions) Inspector General, Department of Defense 400 Army Navy Drive (Room 801) Arlington, VA 22202-2884	**Performing Organization Number(s)** D-2001-016
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	

Abstract

In a memorandum to the Inspector General, DoD, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)expressed concerns that system owners and users may have created increased vulnerabilities to the Defense information infrastructure and to operational readiness during the year 2000 renovation processes. The Assistant Secretary asked the Inspector General, DoD, to monitor the adherence of DoD Components to the information security requirements of the Office of the Secretary of Defense. As of March 2000, the DoD year 2000 database identified 889 renovated mission-critical systems. We conducted the audit in two phases. In phase one, we reviewed DoD policies on the use of identification and authentication controls to access information systems. In phase two, we reviewed security controls at selected locations.

Subject Terms	
Document Classification unclassified	**Classification of SF298** unclassified

Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 35	

Additional Copies

To obtain additional copies of this audit report, visit the Inspector General, DoD, Home Page at www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit of the Audit Followup and Technical Support Directorate 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 Audit Followup and Technical Support Directorate at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

OAIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General, Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-2885

Defense Hotline

To report fraud, waste, or abuse, contact the Defense Hotline by calling (800) 424-9098; by sending an electronic message to Hotline@dodig.osd.mil; or by writing to the Defense Hotline, The Pentagon, Washington, D.C. 20301-1900. The identity of each writer and caller is fully protected.

Acronyms

ASD(C^3I)	Assistant Secretary of Defense (Command, Control, Communication, and Intelligence)
COTS	Commercial-Off-The-Shelf
DITSCAP	DoD Information Technology Security Certification and Accreditation Process
Y2K	Year 2000

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

December 12, 2000

MEMORANDUM FOR ASSISTANT SECRETARY OF THE AIR FORCE
(FINANCIAL MANAGEMENT AND COMPTROLLER)
DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY
DIRECTOR, DEFENSE LOGISTICS AGENCY
DIRECTOR, WASHINGTON HEADQUARTERS SERVICES
NAVAL INSPECTOR GENERAL
AUDITOR GENERAL, DEPARTMENT OF THE ARMY

SUBJECT: Audit Report on Security Controls Over Contractor Support for Year 2000 Renovation (Report No. D-2001-016)

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

We revised the recommendations to require that Component Chief Information Officers assess risk to the security baseline for renovated systems and accredit or reaccredit renovated systems in accordance with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process." We request comments on the final report from the Chief Information Officers of the Army, Navy, Marine Corps, Defense Information Systems Agency, and the Defense Logistics Agency.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. Management comments should indicate concurrence or nonconcurrence with the finding and recommendations. Comments should describe actions taken or planned in response to agreed-upon recommendations and provide the completion dates of the actions. State specific reasons for any nonconcurrence and propose alternative actions, if appropriate. Comments on the final report are due by February 12, 2001.

We appreciate the courtesies extended to the audit staff. For additional information on this report, please contact Ms. Wanda A. Hopkins, at (703) 604-9049 (DSN 664-9049) (wahopkins@dodig.osd.mil) or Ms. Dianna J. Pearson, at (703) 604-9063 (DSN 664-9063) (djpearson@dodig.osd.mil). See Appendix D for the report distribution and the inside back cover for a list of the audit team members.

Robert J. Lieberman
Assistant Inspector General
for Auditing

Office of the Inspector General, DoD

Report No. D-2001-016 **December 12, 2000**
(Project No. D1999AS-0052.01)

Security Controls Over Contractor Support For Year 2000 Renovation

Executive Summary

Introduction. In a memorandum to the Inspector General, DoD, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) expressed concerns that system owners and users may have created increased vulnerabilities to the Defense information infrastructure and to operational readiness during the year 2000 renovation processes. The Assistant Secretary asked the Inspector General, DoD, to monitor the adherence of DoD Components to the information security requirements of the Office of the Secretary of Defense. As of March 2000, the DoD year 2000 database identified 889 renovated mission-critical systems.

We conducted the audit in two phases. In phase one, we reviewed DoD policies on the use of identification and authentication controls to access information systems. In phase two, we reviewed security controls at selected locations.

Objectives. The purpose of the audit was to determine user adherence to DoD information systems security policy during and after year 2000 renovation efforts. In phase one of the audit, we reviewed identification and authentication policy within DoD and issued Inspector General, DoD, Report No. D-2000-058, "Identification and Authentication Policy," December 20, 1999. In phase two, we reviewed implementation of security controls at selected locations. Specifically, we reviewed controls over contractors that performed year 2000 renovations on a sample of 159 mission-critical systems.

Results. DoD Components used techniques, such as access controls, configuration management, and code verification and validation, to monitor and control contractor access to the 159 mission-critical systems in our sample that were renovated by contract personnel during the year 2000 renovation effort. However, the cognizant DoD Components did not assess risk for 103 of those 159 systems and did not reaccredit 119 systems. As a result, at least seven DoD Components were not assured that documented security postures were valid. Further, potential risks to the mission-critical systems were unknown and the systems may be exposed to increased risk of unauthorized access and modification.

Summary of Recommendations. We recommend that the Chief Information Officers of the Army, Navy, Air Force, Marine Corps, Defense Information Systems Agency, Defense Logistics Agency, and Washington Headquarters Services:

- Assess the potential risks to the security baseline requirements for renovated systems for which risk assessments are lacking.

- Accredit or reaccredit renovated systems in accordance with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process."

Management Comments. The Department of the Air Force concurred with the finding and recommendations, and stated that the designated approving authorities will complete security risk assessments and the certification and accreditation process. Washington Headquarters Services has begun to take actions to assess the potential risk to the security baseline for the 20 systems that contractors renovated for the year 2000 and to transition to the DoD Information Technology Security Certification and Accreditation Process. Washington Headquarters Services recognizes the importance of continuously assessing risk and understands that all of its components need to be certified and accredited to maintain the information assurance and security posture of the Defense Information Infrastructure. The Military Traffic Management Command concurred with the report and stated that it was in the process of accrediting or reaccrediting their systems. Refer to the Finding section of the report for the complete discussion of management comments and to the Management Comments section for the complete text of the management comments.

Audit Response. Washington Headquarters Services comments did not indicate a concurrence or nonconcurrence. However, based on actions taken or planned, we consider the comments to be fully responsive.

Management Comments Required. The Army, Navy, Marine Corps, Defense Information Systems Agency, and Defense Logistics Agency did not respond to a draft of this report dated September 21, 2000. Accordingly, we redirected the recommendations to their respective Chief Information Officers. We request comments to the final report by February 12, 2001.

Table of Contents

Introduction

In a memorandum dated May 5, 1999, the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) (ASD [C^3I]) expressed concerns that system owners and users may have created increased vulnerabilities to the Defense information infrastructure and to operational readiness during the year 2000 (Y2K) renovation processes. The ASD (C^3I) asked the Inspector General, DoD, as part of ongoing audits, to monitor DoD Components' adherence to the Office of the Secretary of Defense (OSD) information security requirements and specifically addressed requirements relating to identification and authentication controls outlined in OSD Administrative Instruction (AI) 26-1.

In phase one of this audit, we reviewed DoD Component policies on the use of identification and authentication controls to access information systems. A comparison of the status of Service Component and Defense Agency policies and the requirements of AI 26-1 is discussed in Inspector General, DoD, Report No. D-2000-058, "Identification and Authentication Policy," December 20, 1999.

In phase two, we focused on the application of security controls over contractor-performed Y2K renovations. We selected a sample of mission-critical systems and developed a questionnaire to determine the techniques DoD Components used to monitor and control contractor access during and after Y2K renovations. See Appendix A for a discussion of the sample selection process and the contents of the questionnaire.

Background

The Y2K renovation efforts exposed DoD mission-critical systems to many threats and vulnerabilities. According to the Department of Defense Year 2000 Management Plan, September 1999, Appendix B, the Y2K renovation efforts provided an opportunity to introduce or exploit existing vulnerabilities within any information system or network. Such vulnerabilities could be used to attack the information, information systems, and networks that comprise the DoD information infrastructure and allow opportunities to implant backdoor software routines[1] or malicious code,[2] such as viruses[3] and worms.[4] The Y2K renovation

[1] Backdoors are hidden network utility programs that allow the removal of computer system controls.

[2] Malicious software or code is software written to cause damage or deplete resources of the target computer.

[3] Viruses are software programs that are capable of replication and capable of wreaking great harm on a system. Viruses first copy themselves to additional program files, infect the system programs, and modify the programs to include a possible evolved copy of the virus.

[4] Worms may replicate through an entire network, consuming computer resources, such as memory and bandwidth, and slowing down computers and servers.

process required considerable contractor support and allowed contractors to gain full access to DoD information systems undergoing renovation. The Y2K renovation effort also provided Government personnel, and others associated with Y2K testing and evaluation, with increased access to mission-critical systems.

Year 2000 renovated systems are subject to DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988, which provides for reaccreditation of information technology systems that undergo changes to the associated environment. Additionally, DoD Directive 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, prescribes the security accreditation for information technology systems. The security posture of the defense information infrastructure depends on certifying and accrediting systems for effective information security.

Certification. Certification is the comprehensive evaluation of technical and nontechnical security features of an information system made in support of the accreditation process. Certification establishes the extent that a particular system design and implementation meet specified security requirements.

Accreditation. Accreditation is the formal security declaration by an authorized official to approve the operation of an information technology system or network. The accreditation describes the definitive baseline of security operations and the particular security mode using a prescribed set of safeguards. Accreditation is based on security assumptions that tie certified hardware and software of each system to the configuration of the computing environment.

Objective

The audit objective was to determine user adherence to DoD information systems security policy during and after Y2K renovation efforts. We reviewed implementation of security controls at selected locations. Specifically, we reviewed controls over contractors that performed Y2K renovations on mission-critical systems. See Appendix A for a discussion of the audit scope, methodology, and a summary of prior coverage related to the audit objective.

Certifying and Accrediting Information Systems After Year 2000 Renovation

DoD Components used various security measures, such as access controls, configuration management, and code verification and validation, to control and monitor contractor access to 159 mission-critical systems during the year 2000 (Y2K) renovation process. However, 7 of the 8 DoD Components with systems in our sample did not assess the potential risk related to the renovation efforts for 103 of 159 contractor-renovated systems and did not reaccredit 119 systems. The condition existed because DoD personnel did not adhere to established defense information security policies and procedures relating to system modifications. As a result, DoD Components were not assured that documented security postures were valid. Further, potential risks to the mission-critical systems were unknown and the systems may be exposed to increased risk of unauthorized access or modification.

DoD Mission-Critical Systems

Y2K Contractor-Renovated Mission-Critical Systems. As of March 2000, the DoD Y2K database identified 889 Y2K renovated mission-critical systems. We reviewed a sample of mission-critical systems to determine how DoD monitored and controlled contractor access to the systems during the Y2K renovation process. We focused on 159 systems that were contractor-renovated or renovated using a combination of government and contractor personnel. See Appendix A for details on the DoD Y2K database, the sample selection process, and a description of the sample reviewed. Appendix B provides a list of the 159 systems reviewed and Appendix C provides details on the techniques DoD Components used to monitor contractor renovation of the 159 systems.

Certification and Accreditation Process

DoD Components did not assess the potential risk related to the renovation efforts for 103 of 159 contractor-renovated systems and did not reaccredit 119 systems. The DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," December 30, 1997, outlines the security certification and accreditation process for unclassified and classified information technology. The DITSCAP is composed of four phases: definition, verification, validation, and post accreditation.

The definition phase focuses on understanding the mission, environment, and architecture to determine the security requirements and level of effort required to obtain accreditation and establishes a certification schedule. The agreement is documented in the System Security Authorization Agreement. The verification phase focuses on producing a system that is ready for certification testing, while the validation phase confirms the compliance of the system with the information

contained in the System Security Authorization Agreement. The validation phase provides the evidence required to support the system accreditation. The definition, verification, and validation phases are repeated as often as necessary to obtain an accredited system. The post accreditation phase includes those activities necessary for continuing operation of the accredited system in its environment and to address changing threats. The objective of this phase is to ensure secure system management, operation, and maintenance to preserve an acceptable level of residual security risk. The post accreditation phase continues until the information system is removed from service, a major change is planned for the system, or a periodic compliance validation is required. If the system changes or the periodic validation requires, the DITSCAP process starts over at the definition phase.

Status After Y2K. After Y2K renovations, equipment, architecture, security requirements previously agreed to and documented in the System Security Authorization Agreement were no longer valid. Specifically, DITSCAP requires the Information System Security Officer to determine the extent the changes affect the security posture of either the information system or the computing environment. However, DoD Components did not comply with the DITSCAP to reassess the systems security posture subsequent to modifications made to the mission-critical systems during Y2K.

Risk Assessments and Post-Accreditation

Risk Assessments. Risk assessment and risk management are ongoing efforts that should be performed throughout system development and renovation processes. Risk assessment includes analyzing threats to and vulnerabilities of information systems and the potential impact that the loss of information or capabilities has on national security. The resulting analyses are used to identify appropriate and effective security measures to ensure the protection of information. Risk assessments should also consider data sensitivity and integrity and the range of risks the systems and data may be subject to, including risks posed by authorized internal and external users, and unauthorized outsiders who may try to break into the systems. Additionally, such analyses should include reviews of systems and network configurations and observations and testing of existing security controls. Although DoD Components should periodically perform a formal comprehensive risk assessment, risk should be assessed whenever there is a change in operation, technology, or outside influences. However, on completion of the contractor Y2K renovations, DoD Components completed initial or revised risk assessments for only 56 of the 159 mission-critical systems renovated. Consequently, the DoD Components responsible for the remaining 103 systems were unaware of the risk their systems faced after renovation.

Reaccreditation. Changes in the information system's configuration, operational mission, computer environment, or to the configuration of the computing environment may invalidate the original security assumptions and mandate reaccreditation. Therefore, as a minimum, DoD should reaccredit its automated information system every 3 years and reaccredit the system frequently based on system changes and modifications. Of the 56 mission-

critical systems that received initial or revised risk assessments, DoD Components reaccredited only 40 of those systems after the completion of the contractor Y2K renovations. When asked about the lack of risk assessments, accreditations, and reaccreditations, various DoD Components responded that they were not aware that the process was required or simply stated that the process was not performed. The table below shows the status of risk assessments and reaccreditations of mission-critical systems after the contractor Y2K renovations. However, until all mission-critical systems are accredited or reaccredited, DoD mission-critical systems will remain vulnerable to unknown threats.

Table 1. Status After Y2K Renovation

	Contractor Renovated	Risk Assessments Yes	Risk Assessments No	Reaccreditation Yes	Reaccreditation No
Army	45	25	20	9	36
Navy	34	9	25	9	25
Air Force	16	7	9	7	9
Marine Corps	14	0	14	0	14
DISA	23	15	8	15	8
DLA	7	0	7	0	7
WHS	20	0	20	0	20
Total	159	56	103	40	119

DISA Defense Information Systems Agency
DLA Defense Logistics Agency
WHS Washington Headquarters Services

Conclusion

Despite successful Y2K changes and modifications, more needs to be done to minimize the security risk for renovated systems. All DoD Components that renovated systems for the Y2K conversion should consider the results of this audit and the security posture of those systems.

Recommendations, Management Comments, and Audit Response

Revised and Redirected Recommendations. Based on the responses received, we redirected the recommendation to the respective Component Chief Information Officers.

We recommend that the Chief Information Officers of the Army, Navy, Air Force, Marine Corps, Defense Information Systems Agency, Defense Logistics Agency, and Washington Headquarters Services:

1. Assess the potential risks to the security baseline requirements for renovated systems for which risk assessments are lacking.

2. Accredit or reaccredit renovated systems in accordance with DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process."

Department of the Air Force Comments. The Department of the Air Force concurred with the finding and recommendations. The designated approving authorities for the nine Air Force systems identified in the audit will accomplish security risk assessments by March 1, 2001, and complete the certification and accreditation process by December 1, 2001. The complete text of the Air Force comments can be found in the Management Comments section of the report.

Washington Headquarters Services Comments. Washington Headquarters Services has begun to take actions to assess the potential risk to the security baseline for the 20 systems that contractors renovated for the year 2000 and to transition to the DoD Information Technology Security Certification and Accreditation Process. Washington Headquarters Services recognizes the importance of continuously assessing risk and understands that all of its components need to be certified and accredited to maintain the information assurance and security posture of the Defense Information Infrastructure. The complete text of the Washington Headquarters Services comments can be found in the Management Comments section of the report.

Audit Response. Washington Headquarters Services comments did not indicate a concurrence or nonconcurrence. However, based on actions taken or planned, we consider the Washington Headquarters Services comments to be fully responsive.

Military Traffic Management Command Comments. Although not required to comment, the Military Traffic Management Command concurred with the recommendations and stated that it was in the process of accrediting or reaccrediting their systems. The complete text of the Military Traffic Management Command comments can be found in the Management Comments section of the report.

Audit Response. The Military Traffic Management Command has taken responsive action.

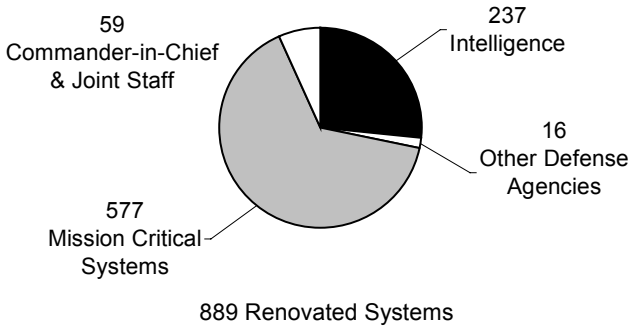
Management Comments Required. The Army, Navy, Marine Corps, Defense Information Systems Agency, and Defense Logistics Agency did not respond to a draft of this report dated September 21, 2000. Accordingly, we redirected the recommendations to their respective Chief Information Officers. We request comments to the final report by February 12, 2001.

Appendix A. Audit Process

Scope

Work Performed. We obtained a list of the DoD mission-critical systems from the DoD Y2K database to determine the number of systems renovated for Y2K. According to the Y2K database as of March 2000, DoD Components identified 889 renovated mission-critical systems. Due to constraints related to resources, time and other factors, we excluded from the sample universe intelligence systems, systems located at the Joint Staff and Commander-in-Chief locations, and DoD Components with less than 10 renovated systems. We identified the locations with the most systems and judgmentally selected a sample of systems at each location. We selected 330 renovated systems for review.

Figure 2. DoD Mission-Critical Systems Renovated for Y2K



Sample Description. We relied on DoD Components to identify contractor-renovated systems, Government-renovated systems, and systems that did not require renovation. We provided a questionnaire for each of the 330 systems. Of the 330 systems identified, 159 systems were contractor-renovated or renovated using a combination of government and contractor personnel, 122 systems were renovated by government personnel, 37 systems were not renovated, and 12 systems were not specifically identified. We reviewed and summarized data pertaining only to the 159 contractor-renovated systems. The questionnaire identified access controls, background checks, configuration management, and code verification and validation as techniques that DoD used to monitor and control contractor access during Y2K renovation. We summarized the responses to determine how each sampled DoD location monitored or controlled contractors used in the Y2K renovation effort.

DoD-Wide Corporate-Level Government Performance and Results Act (GPRA) Coverage. In response to the GPRA, the Secretary of Defense annually establishes DoD-wide corporate-level goals, subordinate performance goals, and performance measures. However, the Secretary of Defense had not established any GPRA goals for Information Assurance.

DoD Functional Area Reform Goals. Most major DoD functional areas have also established performance improvement reform objectives and goals. This report pertains to the achievement of the following functional area objectives and goals:

> **Information Technology Functional Issue Area.**
> **Objective:** Ensure DoD vital information resources are secure and protected. **Goal:** Improve acquisition processes and regulations. **(DoD-5.2) Goal:** Assess information assurance posture of DoD operational systems. **(ITM-4.4)**

General Accounting Office High-Risk Area. The General Accounting Office has identified several high-risk areas in the DoD. This report provides coverage of the Information Management and Technology high-risk area.

Methodology

Audit Type, Dates, and Standards. We performed this economy and efficiency audit from February through August 2000, in accordance with auditing standards issued by the Comptroller General of the United States, as implemented by the Inspector General, DoD.

Use of Computer-Processed Data. To achieve the audit objectives, we relied on computer-processed data contained in the DoD Y2K database. Our review of system controls and the results of data tests showed an error rate that casts doubt on the validity of the data. However, when the data are reviewed in context with other available evidence, we believe that the opinions, conclusions, and recommendations in this report are valid.

Contacts During the Audit. We visited or contacted individuals and organizations within DoD. Further details are available on request.

Management Control Program Review

We did not review the management control program related to the overall audit objective because DoD designated information assurance as a material management control weakness in the FY 1999 Annual Statement of Assurance.

Prior Coverage

General Accounting Office

GAO reports can be accessed over the Internet at http://www.gao.gov.

GAO Report No. T-NSIAD-00-148, "DoD Personnel: Weaknesses in Security Investigation Program Are Being Addressed," April 6, 2000.

GAO Report No. AIMD-00-55, "Computer Security: FAA Needs to Improve Controls Over Use of Foreign Nationals to Remediate and Review Software," December 23, 1999.

Inspector General, DoD

The DoD audit and inspection agencies issued over 200 reports on the DoD Y2K conversion, including about 185 reports by the Inspector General, DoD. In addition, there have been numerous reports on information security matters, although those reports are generally classified or For Official Use Only. The text of the releasable Inspector General, DoD, reports is available on-line at http://www.dodig.osd.mil.

Appendix B. Renovated Systems Sampled

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Army Systems							
1	CCSLA[1]	Army Computer Security Commodity Logistics Accounting Information Management System	X	X			X
2	CECOM[2]	Message Switch (SEC)	X	X			X
3	CECOM[2]	Army Switch Program	X	X			X
4	CECOM[2]	ASAS - All Source (BLOCK I) (SEC)	X	X		X	
5	CECOM[2]	ASAS - Comm Control System (BLOCK I) (SEC)	X	X		X	
6	CECOM[2]	ASAS - Remote Work Station (BLOCK I) (SEC)	X	X		X	
7	CECOM[2]	ASAS - SS/EAC (BLOCK I) (SEC)	X	X		X	
8	CECOM[2]	Cont Central Comp AN/FSC-115, GSC-63 (SEC)	X	X			X
9	CECOM[2]	MLRS - Fire Direction Sys, AN/GYK-37 (SEC)	X		X	X	
10	CECOM[2]	MSE Network Planning Term AN/UYK-100 (SEC)	X		X		X
11	CECOM[2]	System Control Center, AN/TYQ-46(V)2 (SEC)	X	X		X	
12	CECOM[2]	Satellite Configuration Control Element An/FSC-91 (SEC)	X	X			X
13	CECOM[2]	Satellite Communications Set (SCS) (SEC)	X	X			X
14	CECOM[2]	Trailblazer, AN/TSQ-138 (SEC)	X		X		X
15	ILSC[3]	Standard Depot System	X	X			X
16	LOGSA[4]	Army Airlift Clearance Authority	X		X		X
17	LOGSA[4]	Army Total Asset Visibility	X		X		X
18	LOGSA[4]	DoD Address Directory	X		X		X
19	LOGSA[4]	Logistics Intelligence File	X		X		X
20	LOGSA[4]	Unit Movement Visibility	X		X		X
21	LSSC[5]	Commodity Command Standard System	X	X			X
22	STRICOM[6]	Close Combat Tactical Trainer	X	X			X
23	MTMC[7]	Automated Air Load Planning System	X	X			X

Footnotes/Acronyms defined on pages 17 and 18

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Army Systems (cont'd)							
24	MTMC[7]	Asset Management System	X	X			X
25	MTMC[7]	CONUS Freight Management System	X		X		X
26	MTMC[7]	Integrated Booking System	X	X			X
27	MTMC[7]	Integrated Computerized Deployment System	X	X		X	
28	MTMC[7]	Worldwide Port System	X		X		X
29	PEOC3S[8]	AFATDS A97	X		X	X	
30	PEOC3S[8]	Enhanced Switch Operations Program	X	X			X
31	PEOC3S[8]	Global Command and Control System - Army	X	X			X
32	PEOC3S[8]	Global Command and Control System - Army	X	X			X
33	PEOC3S[8]	Integrated Meteorological System (IMETS) Block II	X	X			X
34	PEOC3S[8]	Joint Collection Management Tools	X		X		X
35	PEOC3S[8]	Airborne Reconnaissance Low - COMINT	X		X		X
36	PEOIEW[9]	Airborne Reconnaissance Low - Multifunction	X		X		X
37	PEOIEW[9]	Guardrail/Common Sensor System 1, AN/USD-9D	X		X		X
38	PEOIEW[9]	Guardrail/Common Sensor System 3 AN/USD-9B	X		X		X
39	PEOIEW[9]	Guardrail/Common Sensor System 4, AN/USD-9C	X		X		X
40	PEOSTAMIS[10]	Standard Army Ammunition System-Modernization	X	X		X	
41	PEOSTAMIS[10]	Standard Army Maintenance System - 1 & 2 Rehost (TACCS Replacement)	X		X		X
42	PEOSTAMIS[10]	Standard Army Retail Supply System Gateway	X	X			X
43	PEOSTAMIS[10]	Standard Army Retail Supply System Level 1 Objective	X		X		X
44	PEOSTAMIS[10]	Standard Army Retail Supply System - 2AD	X	X			X
45	PEOSTAMIS[10]	Transportation Coordinators Automated C2 Information System	X		X		X
		Total Army	45	25	20	9	36

Footnotes/Acronyms defined on pages 17 and 18

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Navy Systems							
46	NAVAIR[11]	AN/TPX-42A(V) Air Traffic Control Direct Altitude and Identity Readout	X		X		X
47	NAVAIR[11]	Integrated Voice Communications Switching System (IVCSS)	X		X		X
48	NAVAIR[11]	Airfield Lighting Control System (AFLICS)	X		X		X
49	NAVAIR[11]	AN/ASM-608 IMUTS	X		X		X
50	NAVAIR[11]	Theater Mission Planning Center	X		X		X
51	NAVAIR[11]	Afloat Planning System	X		X		X
52	NAVAIR[11]	Joint Service Imagery Processing System-NAVY	X		X		X
53	NAVAIR[11]	Tactical Automated Mission Planning System	X		X		X
54	NAVAIR[11]	EA-6B TSQ-142 (V5/6) TEAMS Software Release 205.04	X		X		X
55	NAVSEA[12]	Navigation Command and Control System (NAV/C2)	X		X		X
56	NAVSEA[12]	Cooperative Engagement Capability Baseline 2	X		X		X
57	NAVSEA[12]	Advance Combat Direction System BLK 1 (LHD 1, CV 67,69 ONLY)	X		X		X
58	NAVSEA[12]	Advance Signal Processor	X		X		X
59	NAVSEA[12]	AN/BSY-2 Submarine Combat System	X		X		X
60	NAVSEA[12]	CCS REV 5.5	X		X		X
61	NAVSEA[12]	CCS REV 6.3	X		X		X
62	SPAWAR[13]	Ported SNAP I Shipboard Non-Tactical ADP Program	X	X		X	
63	SPAWAR[13]	NALCOMIS IMA	X	X		X	
64	SPAWAR[13]	NALCOMIS OMA	X	X		X	
65	SPAWAR[13]	Food Service Management System	X	X		X	
66	SPAWAR[13]	Automated Travel Order System	X	X		X	
67	SPAWAR[13]	Aviation Maintenance Material Management	X	X		X	
68	SPAWAR[13]	TLMS	X	X		X	
69	SPAWAR[13]	NTCSS-DANA Desk Top Environment	X	X		X	
70	SPAWAR[13]	Ported Snap II Shipboard Non-Tactical ADP Program	X	X		X	
71	SPAWAR[13]	Multilevel Mail Server	X		X		X
72	SPAWAR[13]	NOVA	X		X		X
73	SPAWAR[13]	Integrated Submarine Automated Broadcast Processing System - ASHORE	X		X		X

Footnotes/Acronyms defined on pages 17 and 18

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Navy Systems (cont'd)							
74	SPAWAR[13]	NATO Interoperable Submarine Broadcast System	X		X		X
75	SPAWAR[13]	Integrated Verdin Transmit Terminal	X		X		X
76	NAVSUP[14]	Uniform Automated Data PRCSS SYS	X		X		X
77	NAVSUP[14]	Residual Asset Management	X		X		X
78	NAVSUP[14]	Advanced Tracebility & Control-Navy	X		X		X
79	NAVSUP[14]	UICP Transition	X		X		X
		Total Navy	34	9	25	9	25
Air Force Systems							
80	AFMC[15]	Air Force Key Data Management System	X		X		X
81	AFMC[15]	Joint Tactical Information Distribution System	X		X		X
82	AFMC[15]	Portable Flight Planning Software	X		X		X
83	AFMC[15]	Comprehensive Engine Management System	X	X		X	
84	TRANSCOM[16]	Analysis of Mobility Platform	X	X			X
85	TRANSCOM[16]	Defense Medical Regulating Information System	X		X	X	
86	TRANSCOM[16]	Automated Patient Evacuation System	X		X	X	
87	TRANSCOM[16]	Global Transportation Network	X		X		X
88	AFMC[15]	Execution and Prioritization of Repairs Support System	X	X			X
89	AFMC[15]	Item Manager Wholesale Requisition Process	X		X		X
90	AFMC[15]	Sustainability Assessment Module	X		X		X
91	AFMC[15]	Combat Ammunition System - Air Logistics Center	X	X		X	
92	AFMC[15]	Combat Ammunition System (Base Level)	X	X		X	
93	AFMC[15]	Combat Ammunition System - Command	X	X		X	
94	AFMC[15]	Combat Ammunition System Deployable	X	X		X	
95	AFMC[15]	Cargo Movement Operations System	X		X		X
		Total Air Force	16	7	9	7	9

Footnotes/Acronyms defined on pages 17 and 18

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Marine Corps Systems							
96	USMC[17]	Contract Divisions Document	X		X		X
97	USMC[17]	Publication System	X		X		X
98	USMC[17]	Item Applications	X		X		X
99	USMC[17]	MCLB Automated Information System Transition Router	X		X		X
100	USMC[17]	Material Return Program	X		X		X
101	USMC[17]	Automated Procurement	X		X		X
102	USMC[17]	Technical Data Management	X		X		X
103	USMC[17]	Provisioning Subsystem	X		X		X
104	USMC[17]	Mechanization of Warehouse and Storage	X		X		X
105	USMC[17]	Transportation Management System	X		X		X
106	USMC[17]	Store Accounting Subsystem	X		X		X
107	USMC[17]	Allotment Accounting Subsystem	X		X		X
108	USMC[17]	Asset Tracking for Logistics and Supply System	X		X		X
109	USMC[17]	Essex Replacement System	X		X		X
		Total Marine Corps	14	0	14	0	14
Defense Information Systems Agency							
110	D2[18]	DISN-Telecommunications Management System-C	X		X		X
111	D3[19]	Defense Satellite Communications System	X	X		X	
112	D3[19]	Automatic Digital Network	X		X		X
113	D3[19]	Bosnia C2 Augmentation	X	X			X
114	D3[19]	Defense Red Switch Network	X	X		X	
115	D3[19]	Enhanced Pentagon Capability	X	X		X	
116	D3[19]	Defense Switched Network	X		X	X	
117	D3[19]	Defense Information Systems Network-Integrated Digital Network Exchange	X		X	X	
118	D3[19]	Joint Spectrum Management System (JSMSw)	X	X		X	
119	D3[19]	Frequency Resource Records System DCF	X	X		X	
120	D3[19]	Frequency Resource Records System CCF	X	X		X	
121	D6[20]	Global Command and Control System V.30	X	X		X	
122	D6[20]	Global Command and Control System JOPES Editing Tools	X	X		X	
123	D6[20]	GSSC of Resources and Training System	X	X		X	
124	D6[20]	National C2 System-Massage Handler	X	X			X

Footnotes/Acronyms defined on pages 17 and 18

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Defense Information Systems Agency (cont'd)							
125	D6[20]	Anti-Drug Network	X	X			X
126	D6[20]	Status of Readiness and Training	X	X		X	
127	D6[20]	Common Operating Picture UB 3.0.2.5	X		X	X	
128	DISA[21]	DISA Internal Network	X	X		X	
129	JECPO[22]	DoD Electronic Business Exchange	X	X		X	
130	JITC[23]	Corporate Database for Windows	X		X		X
131	JITC[23]	Database Commitment Accounting System	X		X		X
132	JITC[23]	Microcomputer Message Analysis System - PJIES	X		X		X
		Total Defense Information Systems Agency	23	15	8	15	8
Defense Logistics Agency							
133	DSDC[24]	Standard Automated Management Material (PEDE)	X		X		X
134	DSDC[24]	Mechanization of Contract Administration Services	X		X		X
135	DSDC[24]	Alerts	X		X		X
136	DSDC[24]	Base Operations Support System	X		X		X
137	DSDC[24]	Distribution Standard System	X		X		X
138	DSDC[24]	Defense Reutilization and Marketing Automated Information System	X		X		X
139	DSDC[24]	Defense Fuels Automated Management System	X		X		X
		Total Defense Logistics Agency	7	0	7	0	7
Washington Headquarters Service Systems							
140	C&D[25]	Correspondence Control System	X		X		X
141	C&D[25]	Directives Issuance Tracking System	X		X		X
142	P&S[26]	Adjucation Facility Tracking System	X		X		X
143	P&S[26]	Personnel & Security Database Application	X		X		X
144	P&S[26]	Senior Executive Service Titles	X		X		X
145	P&S[26]	Military Personnel Tracking System - WHS	X		X		X
146	RE&F[27]	Administrative Assignment Rental Management System/ Rental System	X		X		X
147	RE&F[27]	Contract Guard Service	X		X		X

Footnotes/Acronyms defined on pages 17 and 18

	Component Organization	System Name	Contractor Renovated	Risk Assessment Yes	Risk Assessment No	Reaccreditation Yes	Reaccreditation No
Washington Headquarters Service Systems (cont'd)							
148	RE&F[27]	Day Care Tracking System	X		X		X
149	RE&F[27]	Emergency Contract System	X		X		X
150	RE&F[27]	Fund Analysis System	X		X		X
151	RE&F[27]	Inventory Property Management Information System	X		X		X
152	RE&F[27]	Parking Control Applications	X		X		X
153	RE&F[27]	Personnel Action Tracking System	X		X		X
154	RE&F[27]	Phone Record Tracking System	X		X		X
155	RE&F[27]	Pulaski Parking Permit Tracking System	X		X		X
156	RE&F[27]	Reimbursable Project Worksheet	X		X		X
157	RE&F[27]	Reimbursable Work Orders	X		X		X
158	RE&F[27]	SEMD Tracking Systems	X		X		X
159	RE&F[27]	Integrated Property Management Information System	X		X		X
		Total Washington Headquarters Services	20	0	20	0	20
		Total DoD Systems	**159**	**56**	**103**	**40**	**119**

Component Organization Descriptions

1.	CCSLA	CECOM Communications Security Logistics Agency
2.	CECOM	Communications Electronics Command
3.	ILSC	Industrial Logistics Systems Center
4.	LOGSA	Logistics Support Activity
5.	LSSC	Logistics Systems Support Center
6.	STRICOM	Simulation, Training & Instrumentation Command
7.	MTMC	Military Traffic Management Command
8.	PEOC3S	Program Executive Office for Command, Control, and Computers Systems
9.	PEOIEW	Program Executive Office
10.	PEOSTAMIS	Program Executive Office Standard Army Management Information Systems
11.	NAVAIR	Naval Air Command
12.	NAVSEA	Naval Sea Command
13.	SPAWAR	Space & Naval Warfare Systems Command
14.	NAVSUP	Naval Supply Systems Command
15.	AFMC	Air Force Materiel Command

16.	TRANSCOM	Transportation Command
17.	USMC	United States Marine Corps
18.	D2	Command, Control, Communications, Computer and Intelligence
19.	D3	Operations
20.	D6	Engineering and Information
21.	DISA	Defense Information System Agency
22.	JECPO	Joint Electronic Commerce Program Office
23.	JITC	Joint Interoperability Test Command
24.	DSDC	Defense Logistics Agency Systems Design Center
25.	C&D	Correspondence & Directives
26.	P&S	Personnel & Security
27.	RE&F	Real Estate & Facilities

Appendix C. Techniques to Monitor Contractor Renovations

We reviewed various techniques DoD Components used to control or monitor contractor access to the mission-critical systems. These techniques included access controls, configuration management, and independent validation and verification of software changes to prevent or detect code errors, backdoors, viruses, and malicious code. Results of the control techniques are discussed below.

Access Controls

Access controls are the structures, policies, and procedures that provide reasonable assurance that computer resources are protected against vulnerabilities, such as unauthorized modification, disclosure, loss, or impairment. Access controls address logical and physical controls.

Logical Controls. Logical controls use computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification, passwords, or other identifiers that are linked to predetermined system access privileges.

Physical Controls. Physical controls restrict the entry and exit of personnel, equipment, and media from an area, such as an office building, suite, data center, or room containing a local area network server. Examples of physical controls are cipher locks, security badges, and security guards. Inadequate access controls increase the vulnerability of DoD information systems to external and internal sources that could execute unauthorized changes to programs or introduce malicious code. To mitigate internal risk, access controls should include a requirement for a background check.

Access Control Responses. DoD Components responded that 134 of the 159 contractor-renovated systems had access controls. Also, DoD responded that personnel security background checks were completed for 121 systems. Because DoD Components did not always implement access controls or verify that background checks for the contractors were complete or up to date, the effectiveness of the access control was diminished.

Configuration Management

Controls Over Y2K Modifications. DoD Components used configuration management to control modifications to mission-critical system hardware and software to ensure that systems were protected from improper modifications prior to, during, and after Y2K renovation. According to the DoD Y2K Management Plan, DoD Components were required to use configuration

management procedures to document all changes to information systems and their components. Equally important was the need for each agency to assess dependencies and to communicate all changes to the information systems to internal and external users.

Configuration management procedures resulted in the documentation of a system baseline that identified information system hardware, software, firmware components, and external interfaces. Configuration management procedures also provided the foundation for future security evaluations and established a known reference point from which to make future accreditation decisions.

Configuration Control Responses. DoD Components reported using configuration management procedures that ranged from the use of checklists, tools, and sign-in/out sheets to acceptance testing for 150 of the 159 contractor-renovated systems. Although risk mitigation is best accomplished by using multiple control measures, the various Component responses indicate that there is still a DoD-wide weakness in implementing a standard configuration management program. A standard configuration management program should consist of procedures that provide for authorizing, testing, and maintaining software libraries.

Independent Verification and Validation

Independent verification and validation is an independent review of remediated systems to determine whether those systems were Y2K compliant. Independent verification and validation does not replace testing; rather, it is an independent review that aids in testing by detecting uncorrected fields and lines of code. Activities such as code scanning and virus scanning are considered to be independent reviews that assisted in identifying lines of codes that had the potential to be manipulated by internal and external threats.

Code and Virus Scanning. Code scanning can be part of the independent verification and validation process to identify missed date fields, identify invalid date-processing logic, and validate corrected code. Code scanning includes sub-programs or copybooks, performing analysis to remove false positives, reviewing and validating suspected error, and fixing identified true errors. DoD Components also reported that they scanned code to detect viruses in contractor-renovated systems. Virus scanning, however, does not detect logic errors; logic errors should be detected during code scanning.

Code Validation and Verification Responses. DoD Components responded that they used some form of independent verification and validation, code scanning, or virus detection on only 106 systems of the 159 contractor-renovated systems. Measures to prevent or detect code errors, viruses, or other malicious activities cannot provide a level of effectiveness unless used.

Appendix D. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller/Chief Financial Officer)
  Deputy Chief Financial Officer
  Deputy Comptroller (Program/Budget)
  Director, Program Analysis and Evaluation
Under Secretary of Defense for Personnel and Readiness
Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
  Deputy Assistant Secretary of Defense, Chief Information Officer
  Deputy Assistant Secretary of Defense, Security and Information Operations
    Director, Defense-wide Information Assurance Program
Assistant Secretary of Defense (Health Affairs)

Joint Staff

Director, Joint Staff

Department of the Army

Assistant Secretary of the Army (Acquisition, Logistics, and Technology)
Commander, U.S. Army Materiel Command
  Commander, Army Aviation and Missile Command
  Commander, Army Simulation, Training and Instrumentation Command
  Commander, Logistics Support Activity
  Commander, Army Communications-Electronics Command
Director, Military Traffic Management Command
Inspector General, Department of the Army
Auditor General, Department of the Army
Chief Information Officer, Department of the Army

Department of the Navy

Assistant Secretary of the Navy (Manpower and Reserve Affairs)
Commander, Naval Air Systems Command
Commander, Naval Sea Systems Command
Commander, Naval Supply Systems Command
Commander, Space and Naval Warfare Systems Command
Superintendent, Naval Postgraduate School

Department of the Navy (con't)

Naval Inspector General
    Inspector General, Department of the Navy (Audit/Cost Management Division)
    Deputy Naval Inspector General for Marine Corps Matters, Department of the Navy
Auditor General, Department of the Navy
Chief Information Officer, Department of Navy
Chief Information Officer, Marine Corps

Department of the Air Force

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

Unified Commands

Inspector General, U.S. Central Command
Inspector General, U.S. Joint Forces Command
Inspector General, U.S. Pacific Command
Inspector General, U.S. Space Command
Inspector General, U.S. Southern Command
Inspector General, U.S. Special Operations Command

Other Defense Organizations

Defense, Contract Management Agency
Director, Defense Commissary Agency
Director, Defense Contract Audit Agency
Defense, Finance and Accounting Service
Director, Defense Information Systems Agency
    Inspector General, Defense Information Systems Agency
    United Kingdom Liaison Officer, Defense Information Systems Agency
Director, Defense Logistics Agency
Director, National Security Agency
    Inspector General, National Security Agency
Director, Washington Headquarters Services
Director, DoD Human Resources Activity
Inspector General, Defense Intelligence Agency
Inspector General, Defense Threat Reduction Agency
Inspector General, National Imagery and Mapping Agency

Non-Defense Federal Organizations and Individuals

Office of Management and Budget
  Office of Information and Regulatory Affairs

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Management, Information, and Technology, Committee on Government Reform
House Subcommittee on National Security, Veterans Affairs, and International Relations, Committee on Government Reform

Department of the Air Force Comments

DEPARTMENT OF THE AIR FORCE
HEADQUARTERS UNITED STATES AIR FORCE
WASHINGTON DC

DEC 1 2000

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

FROM: HQ USAF/SC
1250 Air Force Pentagon
Washington DC 20330-1250

SUBJECT: Audit Report on Security Controls Over Contractor Support for Year 2000 Renovation, 21 September 2000 (Project No. OAS-0052.01)

This is in reply to your memorandum requesting Assistant Secretary of the Air Force (Financial Management and Comptroller) to provide Air Force comments on subject report.

Finding. Although DoD Components used various techniques to control and monitor contractor access to 159 mission-critical systems reviewed, those components did not reassess the potential risk the contractor Y2K renovations posed to the overall system security posture. Despite successful Y2K changes and modifications, the security postures related to the non-accredited systems have the ability to impact routine operations, prevent authorized users access to defense systems, and impact continuity of operations.

Recommendations

a. Assess the potential risk to the security baseline requirement for 105 renovated systems.

b. Accredit or reaccredit 119 renovated systems in accordance with DoD 5200.40, "DoD Information Technology Security Certification and Accreditation (C&A) Process.

AF/SC Comments: AF/SC (AF Deputy CIO) concurs with the finding and recommendations. DAAs for the nine AF systems identified in audit will accomplish security risk assessments by 1 Mar 01, and complete the C&A process as prescribed in AFI 33-202, Air Force Computer Security , and AFSSI 5024, Air Force C&A Process by 1 Dec 01.

Our point of contact is Mr Barry J. Washington, HQ USAF/SCMI, DSN 425-6172.

WALTER I. JONES, Brig Gen, USAF
Assistant DCS/Communications and Information

Washington Headquarters Services Comments

Final Report Reference

DEPARTMENT OF DEFENSE
WASHINGTON HEADQUARTERS SERVICES
1155 DEFENSE PENTAGON
WASHINGTON, DC 20301-1155

MEMORANDUM FOR OFFICE OF THE INSPECTOR GENERAL, DOD
ATTENTION: DIRECTOR, ACQUISITION MANAGEMENT DIRECTORATE

SUBJECT: Security Controls Over Contractor Support for Year 2000 Renovation (Project No. 0AS-0052.01)

As requested by the Office of the Inspector General, DoD, this is to provide comments to determine user adherence to DoD information systems security policy in the Department of Defense (DoD), specifically those findings concerning Washington Headquarters Services (WHS).

As recommended in the DoD IG draft report, WHS has already begun to take the following actions: 1) to assess the potential risk to the security baseline requirements of the twenty Y2K contractor-renovated systems and 2) to transition WHS components from their current accreditation process (Automated Information Systems Security Plan (AISSP)) to the DoD Information Technology Security Certification and Accreditation Process (DITSCAP).

As a first stage to assessing the risk to the security baseline, WHS reassessed all criticality factors assigned to the Y2K contractor-renovated systems. Of the twenty systems, WHS has determined that only one, Correspondence Control System (CCS), is mission critical. Two systems have been retired. The remaining seventeen should be reclassified as non-mission essential. The non-mission essential systems are comprised of COTS applications (*e.g. database, spreadsheets*) that reside on the component's network infrastructure and pose no additional risk to the overall security posture of the WHS network following Y2K renovation. Attachment 1 is a spreadsheet that shows the reclassification of each WHS Y2K contractor-renovated system, as well as information on each system's purpose, operational status, external interfaces, application types, and firmware requirements.

After the internal review, the Correspondence Control System (CCS) was the only system identified as Mission Critical. Attachment 2 is copy of the risk assessment accomplished to the security baseline for the CCS. It was accredited within its Automated Information Systems Security Plan (AISSP) and WHS plans to reaccredit this mission critical system via the DITSCAP.

WHS has devised a plan to transition its components from their legacy accreditations and, in the process, to reassess the risk to the security baseline of each of its systems, regardless of mission criticality. Currently, WHS is comprised of eight components. Each of these

AUDIT RESPONSE ~~**FOR OFFICIAL USE ONLY**~~

Management agreed to remove marking.

Final Report Reference

Directorates have accredited their individual enclaves using the AISSP. As the legacy accreditations expire, WHS will incrementally transition all of its components to the DITSCAP. The rewrite of the System Security Authorization Agreements (SSAA) have already begun for several of the WHS components and will continue until the entire WHS Boundary is DITSCAP compliant.

WHS recognizes the importance of continuously assessing risk within a system and implementing risk management principles throughout system development and renovation processes. In addition, WHS understands that to maintain the information assurance (IA) and security posture of the Defense Information Infrastructure (DII), all of its components need to be certified and accredited through the DITSCAP.

We appreciate the opportunity to provide comments concerning the DOD IG's observation regarding adherence to DoD information system security policy. If you have any additional questions, please contact Ms. Mary George at 703-604-4580.

D. O. Cooke
Director

Attachments:
1. Correspondence Control System (CCS) Risk Analysis Worksheet
2. Y2K Renovated System Spreadsheet

cc: Mr. Drake

Omitted because of length. Copies will be provided upon request.

AUDIT RESPONSE ~~**FOR OFFICIAL USE ONLY**~~

Management agreed to remove marking.

Army Military Traffic Management Command Comments

DEPARTMENT OF THE ARMY
HEADQUARTERS, MILITARY TRAFFIC MANAGEMENT COMMAND
200 STOVALL STREET HOFFMAN BUILDING II
ALEXANDRIA VA 22332-5000

MTIM (380) 16 Nov 00

MEMORANDUM FOR Inspector General (IG), Department of Defense, Room 600,
400 Army Navy Drive, Arlington, VA 22202-2884

SUBJECT: Security Controls Over Contractor Support For Year 2000 (Y2k) Renovation

1. Concur with recommendations of the DOD IG review.

2. Currently, MTMC is in the process of accrediting or reaccrediting the seven systems that were included in this review.

3. Point of contact for this action is Kimberly S. Quinn, 703-428-2128, DSN 328-2128.

FOR JOHN S. SMITH
Deputy Chief of Staff
for Information Management

Printed on Recycled Paper

Audit Team Members

The Acquisition Management Division Directorate, Office of the Assistant Inspector General for Auditing, DoD, prepared this report.

Thomas F. Gimble
Mary Lu Ugone
Wanda A. Hopkins
Dianna J. Pearson
Richard B. Vasquez
JoAnn Henderson
H. George Cherry
Timothy Cole
Jamal Hall