

Naval Audit Service



Audit Report



Certification and Accreditation of Information Systems within the Marine Corps

This report contains information exempt from release under the Freedom of Information Act. Exemption (b)(6) applies.

~~Do not release outside the Department of the Navy~~
~~or post on non-NAVAUDSVC Web sites~~
~~without prior approval of the Auditor General of the Navy~~

N2011-0047
2 August 2011

Obtaining Additional Copies

To obtain additional copies of this report, please use the following contact information:

Phone: (202) 433-5757
Fax: (202) 433-5921
E-mail: NAVAUDSVC.FOIA@navy.mil
Mail: Naval Audit Service
Attn: FOIA
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Providing Suggestions for Future Audits

To suggest ideas for or to request future audits, please use the following contact information:

Phone: (202) 433-5840 (DSN 288)
Fax: (202) 433-5921
E-mail: NAVAUDSVC.AuditPlan@navy.mil
Mail: Naval Audit Service
Attn: Audit Requests
1006 Beatty Place SE
Washington Navy Yard DC 20374-5005

Naval Audit Service Web Site

To find out more about the Naval Audit Service, including general background, and guidance on what clients can expect when they become involved in research or an audit, visit our Web site at:

<http://secnavportal.donhq.navy.mil/navalauditservices>



DEPARTMENT OF THE NAVY
NAVAL AUDIT SERVICE
1006 BEATTY PLACE SE
WASHINGTON NAVY YARD, DC 20374-5005

7510
N2010-NFA000-0101
2 Aug 2011

MEMORANDUM FOR COMMANDANT OF THE MARINE CORPS

Subj: **CERTIFICATION AND ACCREDITATION OF INFORMATION SYSTEMS WITHIN THE MARINE CORPS (AUDIT REPORT N2011-0047)**

Ref: (a) NAVAUDSVC memo 7510/N2010-NFA000-0101, dated 4 May 10
(b) SECNAV Instruction 7510.7F, "Department of the Navy Internal Audit"

1. The report provides results of the subject audit announced in reference (a). Section A of this report provides our findings and recommendations, summarized management responses, and our comments on the responses. Section B provides the status of the recommendations. The full text of management responses is included in the Appendix.
2. Actions planned by the Commandant of the Marine Corps meet the intent of the recommendations. Recommendations 8 and 9 are closed, and Recommendations 1-7 and 10-12 are open pending completion of the planned corrective actions. The open recommendations are subject to monitoring in accordance with reference (b). Management should provide a written status report on the recommendations within 30 days after each target completion date.
3. Please provide all correspondence to the Assistant Auditor General for Financial Management and Comptroller Audits, XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX, with a copy to the Director, Policy and Oversight, XXXXXXXXXXXX, XXXXXXXXXXXXXXXXXXXX. Please submit correspondence in electronic format (Microsoft Word or Adobe Acrobat file), and ensure that it is on letterhead and includes a scanned signature.
4. Any requests for this report under the Freedom of Information Act must be approved by the Auditor General of the Navy as required by reference (b). This report is also subject to followup in accordance with reference (b).

Subj: **CERTIFICATION AND ACCREDITATION OF INFORMATION
SYSTEMS WITHIN THE MARINE CORPS (AUDIT REPORT N2011-0047)**

5. We appreciate the cooperation and courtesies extended to our auditors.



XXXXXXXXXXXXXXXXXXXX
Assistant Auditor General
Financial Management and
Comptroller Audits

Copy to:
UNSECNAV
DCMO
OGC
ASSTSECNAV FMC
ASSTSECNAV FMC (FMO)
ASSTSECNAV EIE
ASSTSECNAV MRA
ASSTSECNAV RDA
CNO (VCNO, DNS-33, N40, N41)
CMC (ACMC)
DON CIO
NAVINGEN (NAVIG-4)
AFAA/DO

Table of Contents

EXECUTIVE SUMMARY	1
Overview	1
Reason for Audit.....	2
Noteworthy Accomplishments	2
Conclusions	2
Federal Managers’ Financial Integrity Act.....	3
Federal Information Security Management Act	4
Corrective Actions	4
SECTION A: FINDINGS, RECOMMENDATIONS, AND CORRECTIVE ACTIONS	5
Finding 1: Department of Defense Information Assurance Certification and Accreditation Process Requirements.....	5
Synopsis.....	5
Discussion of Details	5
Background	5
Audit Results	6
Recommendations and Corrective Actions	10
Finding 2: Federal Information Security Management Act Reporting	16
Synopsis.....	16
Discussion of Details	16
Background	16
Audit Results	17
Recommendation and Corrective Actions	18
Finding 3: Management Internal Controls	19
Synopsis.....	19
Discussion of Details	19
Background	19
Audit Results	20
Recommendations and Corrective Actions	21
SECTION B: STATUS OF RECOMMENDATIONS	25
EXHIBIT A: BACKGROUND AND PERTINENT GUIDANCE	27
EXHIBIT B: SCOPE AND METHODOLOGY	32
Scope	32
Methodology.....	32
EXHIBIT C: ACTIVITIES VISITED AND/OR CONTACTED	34
APPENDIX: MANAGEMENT RESPONSE FROM COMMANDANT OF THE MARINE CORPS	35

Executive Summary

Overview

Information security and assurance continues to be a high risk and major issue facing the Department of the Navy (DON) information technology community. Information assurance is required by various laws and regulations to ensure information systems and information are secured. Good controls create a healthy operational environment for all systems. Effective information assurance controls reduce risks that impact all systems to minimize loss or misuse of Government resources. Specifically, information assurance addresses unauthorized access, modification of system data, disruption of system operations, and disclosure of sensitive information. Information assurance is key to providing secure, interoperable information management and information technology across the DON enterprise.

There are two mechanisms for reviewing and validating information assurance controls for implemented information systems and supporting enclaves: (1) the Department of Defense (DoD) Information Assurance Certification and Accreditation Process, and (2) the Federal Information Security Management Act. On 28 November 2007, DoD Instruction 8510.01 established the certification and accreditation process to manage the implementation of information assurance controls, and provide visibility of accreditation decisions for DoD information systems. This instruction applies to all DoD-owned and controlled information systems that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity. In 2002, the Federal Information Security Management Act permanently authorized and strengthened the information security evaluation and reporting requirements established by the Government Information Security Reform Act. The three major requirements discussed in the Federal Information Security Management Act report are: (1) annual security reviews; (2) annual security testing; and (3) contingency plans.

The DoD Information Technology Portfolio Repository is a database that is directly updated by the components, and contains key information that catalogues DoD information systems. The DON variant of the repository is the single, authoritative source for data regarding DON information technology systems, including national security systems. Registration of information systems in DON's repository is central to establishing an accurate enterprise-wide inventory. Also, information in DON's repository is used to meet certification, accreditation, and security management Act reporting requirements. This information is sent to the Office of the Secretary of

Defense, and ultimately, Congress. Therefore, it is critical that data entered into DON's repository is complete and accurate.

The audit evaluated Marine Corps compliance with certification and accreditation requirements and security management Act reporting standards. We judgmentally selected 60 systems from the 152 Marine Corps information systems listed in DON's repository as of 12 May 2010 (see Exhibit B: Scope and Methodology) to determine whether: (1) Marine Corps information systems complied with certification and accreditation requirements, and (2) commands accurately reported Federal Information Security Management Act data elements for Congressional review. To accomplish our audit, we obtained and examined certification and accreditation packages, held discussions with key personnel, and reviewed certification and accreditation procedures. We also evaluated compliance with regulatory requirements and assessed management internal controls within the Marine Corps.

Reason for Audit

The audit objective was to verify that Marine Corps information systems comply with DoD Information Assurance Certification and Accreditation Process requirements, and provide accurate data to meet Federal Information Security Management Act reporting standards.

This audit was requested by the DON Chief Information Officer. The DON Chief Information Officer identified information security and assurance as a top priority in the Fiscal Year (FY) 2009 Risk and Opportunity Assessment data call submission.

Noteworthy Accomplishments

Marine Corps Systems Command and Headquarters Marine Corps are working together to improve the Marine Corps' certification and accreditation process. For example, Marine Corps Systems Command recently implemented the use of the Xacta Information Assurance Manager Assessment Engine (Xacta). Additionally, the Marine Corps has taken action to complete the required certification and accreditation documentation for its information systems.

Conclusions

Marine Corps information systems are not compliant with the certification, accreditation, and security management Act requirements. Although our audit did not reveal compromises of or data manipulation in the 152 information systems of record, we observed several weaknesses in adhering to the DoD Information Assurance Certification

and Accreditation Process and Federal Information Security Management Act reporting. Specifically, our examination of 60 information systems identified the following weaknesses: (1) 58 of the 60 had incomplete certification and accreditation packages; (2) 49 of the 60 were accredited without a certification letter; (3) 13 of the 60 were authorized without an accreditation letter; (4) 13 of the 60 had expired accreditation (authority to operate); and (5) 100 percent of the 60 systems reported security management Act data elements that were incomplete, inaccurate, and/or unsupported.

In addition, the audit disclosed management internal control weaknesses in the following areas: (1) use of an automated certification and accreditation tool; (2) use of an unauthorized accreditation designation; (3) non-compliance with the DoD Reciprocity Agreement; (4) unregistered information systems; and (5) outdated Marine Corps guidance.

Communication with Management. Throughout the audit, we kept senior management officials, including the Marine Corps activities, informed of the conditions noted.

We held opening and closing conferences with Headquarter Marine Corps on 21 April 2010 and 18 November 2010, respectively. During the meetings, we briefed the audit background, scope and methodology, criteria, plans for site visits, and audit milestones. On 18 November 2010 we held a closing conference and communicated with the Marine Corps Senior Information Assurance Official on the results of our audit.

During site visits, from 25 May 2010 through 18 November 2010, we met with the appropriate personnel in the Information Assurance offices including the Designated Accrediting Authority for the U.S. Marine Corps, Certifying Authority, and Information Assurance Managers. We also kept the management officials at each activity informed of the issues we identified involving certification and accreditation of Marine Corps information systems during exit briefings. The audit was conducted at Quantico, VA; and Arlington, VA.

Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act of 1982, as codified in Title 31, United States Code, requires each Federal agency head to annually certify the effectiveness of the agency's internal and accounting system controls. Recommendations 1 through 11 address issues related to the internal controls over the DoD Information Assurance Certification and Accreditation Process and Federal Information Security Management Act. In our opinion, the weaknesses noted in this report may warrant reporting in the Auditor General's annual Federal Managers' Financial Integrity Act memorandum identifying management control weaknesses to the Secretary of the Navy.

Federal Information Security Management Act

The Federal Information Security Management Act of 2002 permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000, which expired in November 2002. Under the provisions of the security management Act, DoD must provide Congress with an annual report on its information assurance posture. The DON Chief Information Officer submits DON input for the DoD security management Act report. Additionally, the security management Act requires an annual independent evaluation of an agency's information security program and practices to determine their effectiveness. The evaluation required by this section may be based in whole or in part on an audit, evaluation, or report relating to programs or practices of the applicable agency. The DON Chief Information Office can use this report in partially meeting that requirement.

Corrective Actions

We made recommendations to the Commandant of the Marine Corps to correct the noted conditions. Specifically, we recommended that the Marine Corps comply with the DoD Information Assurance Certification and Accreditation Process and establish management internal controls and enforcement mechanisms to ensure that certification and accreditation documentation is appropriate, complete, and maintained. We also recommended that oversight processes be put in place to ensure timely recertification and reaccreditation, and consistent use of the Xacta tool. Further, we recommended that the Marine Corps establish management internal controls to ensure that Federal Information Security Management Act data elements are complete, supported, and accurately posted in the DON variant of the DoD Information Technology Portfolio Repository. Additionally, we recommended that the Marine Corps establish (or strengthen existing) management internal controls to address Marine Corps oversight and adherence to DoD policies regarding reciprocity and monitoring of operational information systems.

Actions planned by the Commandant of the Marine Corps meet the intent of the recommendations. Recommendations 8 and 9 are closed, and Recommendations 1-7 and 10-12 are open pending completion of the planned corrective actions.

Section A:

Findings, Recommendations, and Corrective Actions

Finding 1: Department of Defense Information Assurance Certification and Accreditation Process Requirements

Synopsis

The Marine Corps' information systems did not comply with the Department of Defense (DoD) Information Assurance Certification and Accreditation Process, which requires certification and accreditation of all information systems. We found that many of the information systems we looked at were missing key information in accordance with guidance. We also found that the Marine Corps was not using their certification and accreditation tool, Xacta.¹ Further, we found several systems which were inappropriately given accreditation. These conditions occurred because Headquarters Marine Corps had not implemented effective management internal controls, enforcement, and oversight to bring its certification and accreditation program into compliance with DoD guidance. As a result, there is an increased risk of breach, compromise, or the manipulation of data.

Discussion of Details

Background

The DoD Information Assurance Certification and Accreditation Process was implemented to create standardization across the entire DoD. Issued on 28 November 2007, the certification and accreditation process evaluates information assurance principles and controls to ensure that they provide adequate protection for our information technology assets. As the overarching certification and accreditation process for DoD, this process validates security requirements, examines implemented safeguards, and identifies any inadequacies. Proper use of the certification and accreditation methodology will assure Marine Corps leadership that an appropriate level of security is implemented, sufficient controls are in place to adequately protect assets, and the information systems are operating at an acceptable level of residual risk. The Marine

¹ The Xacta Information Assurance Manager assessment engine (Xacta) was established to provide the Marine Corps with a uniform method to complete certification and accreditation in accordance with certification and accreditation process regulations. It was implemented in 2009 and was designed with a series of checks and balances to prevent information systems from receiving certification recommendations and accreditation decisions without completed certification and accreditation packages.

Corps' implementation of the certification and accreditation process provides visibility into information assurance capabilities and services, facilitates collaboration among the stakeholders, and speeds the decision to authorize the operation of a given information system. The certification and accreditation process ensures that adequate security measures are in place to protect information that resides on Department of the Navy (DON) networks. This process is applicable to all DON systems under development and those already in use.

To verify that Marine Corps information systems complied with certification and accreditation process requirements, we used data from the DoD Information Technology Portfolio Repository-Department of the Navy to select activities and information systems to be audited. As of 12 May 2010, the Marine Corps had 152 systems listed in the DON repository. We judgmentally selected 60 of these systems from 4 Marine Corps activities to determine whether they were properly certified and accredited. The systems selected represented the following commands: 28 from Marine Corps Systems Command; 13 from Marine Corps Logistics Command; 11 from Headquarters, Marine Corps; and 8 from Marine Corps Community Services.

Audit Results

Incomplete Certification and Accreditation Packages

We reviewed certification and accreditation documentation, and interviewed personnel overseeing Marine Corps information systems. While 2 of the 60 systems audited complied with the certification and accreditation documentation requirements for certification packages, 58 (97 percent) Marine Corps information systems did not. DoD Instruction 8510.01 requires that the certification and accreditation package consists of a System Identification Profile, an Implementation Plan, a Scorecard, and an Information Technology Security Plan of Action and Milestones. However, of the 58 systems:

- 35 did not have a System Identification Profile. This profile is the set information gathered during system registration that allows unique system identification. System registration establishes the relationship between the system owner and the Chief Information Officer that should continue until the system is decommissioned;
- 45 did not have an Implementation Plan. This plan details the specific information assurance controls (i.e., management, personnel, operational, and technical controls) applied to each DoD information system. The plan also describes the overall system and how the information assurance controls will be implemented and tested to achieve an appropriate level of security;

- 57 did not have a Scorecard. This scorecard provides the results of independent testing of information assurance controls to support accreditation. The Scorecard is intended to convey information about the information assurance posture in a format that can be easily understood; and
- 55 did not have an Information Technology Security Plan of Action and Milestones. This plan is continuously updated as system risks are identified and corrective actions are performed to maintain accreditation during the system life cycle.

The certifying authority is required to have a complete certification and accreditation package in order to make a certification decision and accreditation recommendation. The 58 systems audited were operating without completing the certification and accreditation packages to support the accreditation decisions issued. The Marine Corps management internal controls were not sufficient to ensure that these systems had completed all certification and accreditation process required documentation prior to systems receiving a certification decision.

Ineffective use of Xacta may have allowed 58 systems to receive an accreditation decision and operate without evidence that the required documentation was completed. Issuing an accreditation for information systems that have not completed the certification and accreditation process potentially exposes the Marine Corps to unacceptable levels of risk.

Accreditation without a Certification Letter

Of the 60 systems we reviewed, 49 Marine Corps information systems were assigned an accreditation without a certification determination/recommendation letter. The remaining 11 systems had certification letters, but the dates documented by the commands did not match the dates posted in the DON repository. The DON repository-listed certification dates for each information system differed from documentation provided by the commands from 3 to 341 days. The Designated Accrediting Authority was not in compliance with DoD Instruction 8510.01 when he granted accreditation to information systems without the required certification letter that shows information assurance controls were implemented, tested, and validated to the point where the residual risk is acceptable.

According to DoD Instruction 8510.01, the certifying authority formally states (in a letter) the degree to which a system complies with assigned information assurance controls based on validation results. The certification letter identifies and assesses the residual risk with operating a system and the costs to correct, or mitigate information assurance security weaknesses. The instruction also states that “a certification determination is always required before an accreditation decision” from the Designated

Accrediting Authority. However, Marine Corps management internal controls were not sufficient to identify missing certification letters.

While the Marine Corps mandated Xacta in 2009 to provide visibility, ensure standardization, and automate the certification and accreditation process, the commands we visited either did not use the tool or did not use the tool effectively. The Xacta tool would require the certifying authority to issue a certification recommendation based on the analysis of required certification documentation. Operating information systems that have not completed the certification and accreditation process increases the risk of weaknesses and vulnerabilities, and may jeopardize the success of Marine Corps missions.

Authorization without Accreditation Letter

Of the 60 systems we reviewed, 13 Marine Corps information systems did not have documentation to support accreditation. The DON DoD Information Assurance Certification and Accreditation Process Handbook requires the Designated Accrediting Authority to sign an accreditation letter regarding acceptance of the risk associated with operating a system. However, the Marine Corps management did not have sufficient management internal controls in place to ensure that every information system had an accreditation letter on file. The Marine Corps did not provide an explanation regarding the missing accreditation letters. When DoD systems users connect to DON networks, they trust that Navy and Marine Corps information systems have the proper safeguards in place to protect against potential data corruption. Unaccredited systems may jeopardize the security of the Marine Corps network, which presents a threat to all DoD missions.

Expired Accreditation

Of the 60 systems, 13 Marine Corps information systems were operating with expired accreditation (i.e., Authorization to Operate or Interim Authority to Operate). Office of Management and Budget Circular A-130 states that “an information system must be recertified and reaccredited once every three years. The results of the annual review or a major change in the Information Assurance posture may also indicate the need for recertification and reaccreditation of the information system.” Additionally, Secretary of the Navy Manual 5239.1 “Information Assurance Manual” states, “All DON information systems must be certified and accredited before they can be used.”

However Marine Corps management did not have sufficient management internal controls to identify information systems approaching accreditation expiration and thus re-certify the system before expiration. The Xacta tool was designed to provide command personnel with notifications about systems approaching expiration. While the Marine Corps mandated the Xacta tool in 2009 to provide visibility, ensure standardization, and automate the certification and accreditation process, the commands

we visited either did not use the tool or did not use the tool effectively. Untimely reaccreditation exposes information systems to potential compromise, which may weaken the security of the Marine Corps network.

Inconsistent Use of Xacta

The Xacta tool was used ineffectively and inconsistently at Marine Corps commands. Review of certification and accreditation documentation, and interviews of personnel concluded that Xacta was used inconsistently, and certification and accreditation packages were not completed uniformly. Marine Corps Bulletin 5239 (dated 20 March 2009) states, “Effective immediately, program managers and system owners of information systems and networks will utilize the Xacta to assist in the creation and submission of [certification and accreditation] documentation.” The Marine Corps does not have standard operating procedures in place that detail how Xacta should be used by command personnel. The Marine Corps certification and accreditation personnel relied on the DON DoD Information Assurance Certification and Accreditation Process Handbook, which does not detail how the process should be performed and documented in adherence to certification and accreditation process guidance. The inconsistent use of Xacta, and lack of standard operating procedures has impeded standardization of the certification and accreditation process and hindered the Marine Corps’ ability to certify and accredit their information systems in a timely manner.

Unauthorized Accreditation Designation

Forty-four of the 152 Marine Corps information systems listed in the DON repository were given an accreditation designation that was not established by DoD Instruction 8510.01. The 44 information systems were granted a 1-year designation of “limited authority to operate;” however, this designation is not one of the four accreditation decisions in the instruction. According to the instruction, authorized accreditation decisions are to be expressed as: (1) “authorization to operate”; (2) “interim authorization to operate”; (3) “interim authorization to test”; and (4) “denial of authorization to operate.” However, on 14 July 2009, the Designated Accrediting Authority signed a blanket accreditation letter granting the 44 systems an unauthorized designation of “limited authority to operate.”

The letter was a stop-gap measure to provide command personnel 1 year to complete the required certification and accreditation process because the systems were approaching expiration. Command personnel did not have adequate internal controls in place to ensure that systems were reaccredited prior to expiration. According to the Designated Accrediting Authority, the “limited authority to operate” was granted because security controls were tested and residual risk was within acceptable limits for each of the information systems to operate on the Marine Corps network. However, the Designated

Accrediting Authority was not able to provide documentation to show testing of information assurance controls was performed.

The “limited authority to operate” accreditation letter established the following Headquarters Marine Corps, Command, Control, Communications and Computers approval time tables: (1) Information Technology Security Plan of Action and Milestones in 30 days; (2) DoD Information Assurance Certification and Accreditation Process Implementation Plans in 60 days; and (3) DoD Information Assurance Certification and Accreditation Process packages in 90 days. During the audit, we requested the required certification and accreditation process documentation for the information systems listed on the letter, but command personnel were unable to show compliance with the letter or the certification and accreditation process. Additionally, the 44 information systems were incorrectly reported in the DON repository with an “authority to operate” designation. A system is considered unaccredited if it does not have an authorized accreditation decision. The Marine Corps is operating unaccredited information systems and posting inaccurate information regarding the certification and accreditation status of these systems in DON repository. It is important to note that other DoD components access Marine Corps information system platforms based on information posted in the DON repository. The operation of unaccredited information systems potentially exposes the Marine Corps and other DoD components to unacceptable levels of risk and vulnerability.

Recommendations and Corrective Actions

Our recommendations, summarized management responses, and our comments on the responses are presented below. The complete text of the management responses is in the Appendix.

We recommend that the Commandant of the Marine Corps:

Recommendation 1. Establish controls and governance to ensure that certification and accreditation packages are complete and contain the required Department of Defense Information Assurance Certification and Accreditation Process documentation to support accreditation.

Commandant of the Marine Corps response to Recommendation 1. Concur. The Marine Corps had established controls and governance in place at the time of the audit (e.g., Enterprise Information Assurance Directive 018 – “Marine Corps Certification and Accreditation Process”) as well as numerous Marine Corps Administrative messages; however, there was no process in place to validate and enforce policies or to implement appropriate consequences for instances when compliance was not found. The Marine Corps will update Enterprise Information Assurance Directive 018 with specific requirements, responsibilities, and

standards – including specific consequences for compliance failure. The directive is currently in staffing and will be coordinated, then presented at the next Marine Corps Cybersecurity Conference by 5 August 2011. A final version will be signed by the Director, Command, Control, Communication, and Computers by 1 September 2011; the target completion date for corrective actions in response to Recommendation 1 is 1 September 2011.

Naval Audit Service comment on the response to Recommendation 1.

Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 2. Establish management internal controls to ensure that information systems have appropriate documentation to support the certifying authority's certification recommendation prior to issuing an accreditation.

Commandant of the Marine Corps response to Recommendation 2. Concur. The Marine Corps had controls in place to require documentation and certification authority recommendations for accreditation; however, there are other certification authority representatives throughout the Marine Corps, e.g., Communications Electronics Division officers at base, posts, and stations, who can also provide recommendations for accreditation. The Senior Information Assurance Official, as noted in Department of Defense Instruction 8510.01 – Department of Defense Information Assurance Certification and Accreditation Process, is the service certification authority. According to the Instruction, the Senior Information Assurance Official can also function as the accrediting official (Designated Accrediting Authority). This is the case with the Marine Corps. Some certification authority responsibility was delegated to the Technical Director at Marine Corps Systems Command; however, there were times when mission expediency, combined with independent scans and assessments, were sufficient to make an accreditation decision. The current rewrite to Enterprise Information Assurance Directive 018 will ensure that documentation from the delegated certifying authority and the distributed certification authority representatives are standardized through the use of the current automated Certification and Accreditation document repository in the Xacta automated tool. The Enterprise Information Assurance Directive 018 will be finalized and signed by the Director, Command, Control, Communication, and Computers by 1 September 2011; the target completion date for corrective actions in response to Recommendation 2 is 1 September 2011.

Naval Audit Service comment on the response to Recommendation 2.

Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 3. Establish enforcement mechanism(s) to ensure that certified information systems have a formal accreditation letter to document the Designated Accrediting Authority's designation.

Commandant of the Marine Corps response to Recommendation 3. Concur. The mandated use of the Xacta automated tool ensures all information systems in the Marine Corps have an audit trail of appointments, recommendations, and approvals. All instances of alternate documentation procedures have been directed to be halted and accreditation actions to be accomplished in the automated tool. This will be included in the Enterprise Information Assurance Directive 018, estimated to be signed by the Director, Command, Control, Communication, and Computers by 1 September 2011; the target completion date for corrective actions in response to Recommendation 3 is 1 September 2011.

Naval Audit Service comment on the response to Recommendation 3. Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 4. Establish enforcement mechanism(s) to ensure that the oversight process identifies Marine Corps information systems approaching expired accreditation and timely recertification and reaccreditation prior to expiration.

Commandant of the Marine Corps response to Recommendation 4. Concur. Enterprise Information Assurance Directive 018 will include timeline requirements for scheduled reviews based on expiration dates vice arbitrary schedules. The metric of success will be measured by the Federal Information Security Management Act quarterly and annual approval-to-operate scores. The process and documentation will be tracked in the Xacta automated tool. The Enterprise Information Assurance Directive 018 will be finalized and signed by the Director, Command, Control, Communication, and Computers by 1 September 2011; the target completion date for corrective actions in response to Recommendation 4 is 1 September 2011.

Naval Audit Service comment on the response to Recommendation 4. Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 5. Establish enforcement mechanism(s) and standard operating procedures to ensure that Marine Corps commands are consistently using Xacta as prescribed by Marine Corps Bulletin 5239.

Commandant of the Marine Corps response to Recommendation 5. Concur. Enterprise Information Assurance Directive 018 will codify the mandatory use of the Xacta automated tool by including the wording from the Marine Corps Bulletin and previous Marine Corps Administrative Messages on the topic. At present, no other documentation process (e.g., Information Assurance Control Implementation Determination) is authorized or being used to accredit Marine Corps systems. The Enterprise Information Assurance Directive 018 will be finalized and signed by the Director, Command, Control, Communication, and Computers by 1 September 2011; the target completion date for corrective actions in response to Recommendation 5 is 1 September 2011.

Naval Audit Service comment on the response to Recommendation 5. Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 6. Comply with the Department of Defense Information Assurance Certification and Accreditation Process by issuing approved and recognized accreditation designations to Marine Corps information systems.

Commandant of the Marine Corps response to Recommendation 6. Concur. All accreditation documentation [reviewed during the audit] was in accordance with Department of the Navy and Department of Defense policy. The Designated Accrediting Authority has always been authorized to outline restrictions, limitations, and conditions of accreditation, to ensure the systems' owners and program managers understand the boundaries and requirements to operate securely and with an acceptable level of risk. Titles/designations will be standardized to prevent confusion for anyone not familiar with the Certification and Accreditation process, and to ensure consistent tracking of accreditation documentation. Approved and recognized accreditation designations will be included in the Enterprise Information Assurance Directive 018, estimated to be signed by the Director, Command, Control, Communication, and Computers by 1 September 2011; the target completion date for corrective actions in response to Recommendation 6 is 1 September 2011.

Naval Audit Service comment on the response to Recommendation 6. Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 7. Obtain the required documentation for the 44 systems that were given the "limited authority to operate" designation, and ensure that all elements of the Department of Defense Information Assurance Certification and Accreditation Process are met.

Commandant of the Marine Corps response to Recommendation 7. Concur. All accreditation documentation [reviewed during the audit] was in accordance with Department of the Navy and Department of Defense policy. The Designated Accrediting Authority has always been authorized to outline restrictions, limitations, and conditions of accreditation, to ensure the systems' owners and program managers understand the boundaries and requirements to operate securely and with an acceptable level of risk. Titles/designations will be standardized to prevent confusion for anyone not familiar with the Certification and Accreditation process, and to ensure consistent tracking of accreditation documentation. This will be included in the Enterprise Information Assurance Directive 018, estimated to be signed by the Director, Command, Control, Communication, and Computers by 1 September 2011. The particular systems in question by this audit have been issued Denial of Approval to Operate memos, and are now in the process of going through the reaccreditation process through Xacta. Systems will be re-accredited by 15 September 2011 or they will continue to be under the Denial of Approval to Operate and disconnected. The target completion date for corrective actions in response to Recommendation 7 is 15 September 2011.

Naval Audit Service comment on the response to Recommendation 7. Commandant of the Marine Corps' planned actions to issue system's Denial of Approval to Operate memos, reaccredit the 44 systems, use standard title and designations to clarify the Certification and Accreditation process, track accreditation documentation, and issue guidance on system's certification and accreditation meets the intent of recommendation. We consider this recommendation open pending completion of agreed-to actions.

Commandant of the Marine Corps additional technical comments. With respect to the comments on page 9 and 10 of the draft report, which stated the Designated Accrediting Authority was not able to provide documentation to show testing of information assurance controls, the Marine Corps completes monthly security scans for all systems, as well as Web site scans. Scan reports covering at least the last 2 years are in a repository and are made available, and each report shows analysis regarding Information Assurance Vulnerability Alert implementation and security configuration. In addition, the Marine Corps Network Operations and Security Center sends scanning and security reports to the Joint Task Force-Global Network Operations, which are available for review on their portal. Based on these reports, the Designated Accrediting Authority can, and has been able to, make a risk-based decision regarding the security operations within the Marine Corps enterprise. While the Marine Corps will continue to ensure that documented certification recommendations are provided, the Designated Accrediting Authority had, and continues to have, sufficient information to accept risk and approve systems for operations, even in the few cases where there may be little to no documented certification recommendations.

Naval Audit Service response to Marine Corps additional technical comments.

During our review, the auditors determined that Marine Corps information systems were operating under an unauthorized accreditation designation. The Designated Accrediting Authority provided “limited authority to operate” to 44 information systems that were approaching expiration. This unauthorized accreditation designation was a stop-gap measure to give command personnel 1 year to complete Department of Defense Information Assurance Certification and Accreditation Process packages to obtain accreditation. One component of the Department of Defense Information Assurance Certification and Accreditation Process package is the “scorecard,” which documents the results from implementation and testing of required baseline information assurance controls. This report stated the Designated Accrediting Authority was not able to provide documentation to show testing of information assurance controls because information systems were missing Department of Defense Information Assurance Certification and Accreditation Process scorecards. In the absence of scorecards, the Designated Accrediting Authority based his accreditation decision on monthly security scans performed. While the scans are meant to provide a level of confidence regarding the security posture of Marine Corps information systems; Department of Defense guidance requires that results of implementation of required baseline information assurance controls be documented in the Department of Defense Information Assurance Certification and Accreditation Process scorecard. Additionally, during the 1-year timeframe, none of the 44 systems completed the certification and accreditation process to receive accreditation.

Finding 2: Federal Information Security Management Act Reporting

Synopsis

Our examination determined that Marine Corps commands did not provide accurate information for Federal Information Security Management Act reporting to Congress. For our audit, we judgmentally selected 60 of the 152 Marine Corps information systems listed on the Department of Defense Information Technology Portfolio Repository-Department of Navy. For the 60 systems audited, the Marine Corps could not provide documentation to support security management Act data elements reported in the DON repository. These conditions existed because management internal controls were not sufficient to ensure that data elements complied with the Act's reporting requirements. Specifically, we identified the following weaknesses: (1) incomplete security management Act data elements and (2) unsupported/inaccurate information reported in the DON repository. Failure to complete required data elements for security management Act reporting increases the risks of breach or manipulation to Marine Corps information systems and potentially compromises the safety of the war fighters. Additionally, reporting inaccurate security management Act requirements may adversely affect Congressional funding levels for the next fiscal year.

Discussion of Details

Background

The Federal Information Security Management Act permanently authorized and strengthened the information security program, evaluation, and reporting requirements established by the Government Information Security Reform Act. The three major requirements discussed in the security management Act reports are: (1) annual security reviews; (2) annual security testing; and (3) contingency plans.

The security management Act specifically calls for agencies to design policies and procedures that ensure that information security is addressed throughout the lifecycle of an information system, and not simply as a final, quality control procedure performed prior to deployment. The Act also requires agencies to draft plans that describe security measures that address specific system requirements and comply with policies and procedures. This Act calls for the evaluation of policies, procedures, and practices through annual testing of every information system on the agency's inventory. Additionally, the Act requires that these tests are performed as often as necessary, based on the amount of risk such systems are designed to protect, but at least once a year. It further requires the testing of operational controls. Lastly, the Act requires every information system on the agency's inventory to be subject to a documented plan

containing procedures to ensure continuity of system operations in the event of a failure or system corruption. As part of the operational security controls for the system, such plans must also be tested annually.

Audit Results

Incomplete Federal Information Security Management Act Data Elements

Our audit of 60 Marine Corps information systems disclosed that the 60 systems did not have all of the data elements (annual security reviews, annual security control testing, and contingency plans) required by the security management Act. Of the 60 information systems: 55 had not completed annual security reviews; 59 did not have an approved contingency plan; and none completed the annual security controls testing. These conditions existed because management internal controls were not sufficient to ensure that data elements complied with the Act's reporting requirements. According to Secretary of the Navy Manual 5239.1, the annual Federal Information Security Management Act report summarizes the data in the DON repository, including the certification and accreditation status of systems, dates of annual reviews, and dates of annual testing of security controls and contingency plans. The completion of security management Act data elements is critical as a preventative measure to secure Federal information systems from unauthorized users, and restore data after a disruption. These statistics play an important part in Congress' annual grading of Federal agency information systems' security programs. Reporting incomplete data elements to Congress may adversely affect Marine Corps budgetary funding.

Unsupported/Inaccurate Information in the DoD Information Technology Portfolio Repository-DON

The Federal Information Security Management Act data elements for 54 of the 60 systems posted in the DON repository were unsupported and/or inaccurate. For each information system, we compared the DON repository data to documentation provided by the commands to determine that the Marine Corps could not provide documentation to support dates posted in the DON repository. For the remaining six systems (10 percent), the dates listed on documentation provided by commands did not match dates posted in the DON repository. This condition existed because the Marine Corps did not have management internal controls in place to ensure that data elements were supported and posted accurately in DON repository. According to Secretary of the Navy Manual 5239.1, the annual security management Act report summarizes the data in the DON repository, including: the certification and accreditation status of systems, dates of annual reviews, and dates of annual testing of security controls and contingency plans. Congress requires reporting of dates when data are reviewed and/or tested. Operating information systems without security management Act-required evidence of reviews and testing may

expose the Marine Corps network to unacceptable levels of risk or vulnerability. Also, posting inaccurate information in the DON repository adversely impacts Congress' assessment of the DON's security posture and funding needs.

Recommendation and Corrective Actions

Our recommendations, summarized management responses, and our comments on the responses are presented below. The complete text of the management responses is in the Appendix.

We recommend that the Commandant of the Marine Corps:

Recommendation 8. Establish management internal controls to ensure that data elements are completed in compliance with Federal Information Security Management Act reporting standards, are supported, and accurately posted into the Department of Defense Information Technology Portfolio Repository-Department of the Navy.

Commandant of the Marine Corps response to Recommendation 8. Concur. The newly created Headquarters Marine Corps Command, Control, Communication, and Computers Chief Information Officer Division supports the Marine Corps Chief Information Officer with maintaining and supervising Department of Defense Information Technology Portfolio Repository-Department of the Navy policy. Headquarters Marine Corps Command, Control, Communication, and Computers Cybersecurity Division has the responsibility to ensure the Federal Information Security Management Act tab to Department of Defense Information Technology Portfolio Repository-Department of the Navy is updated with appropriate artifacts in a timely manner. Policies have been implemented by Headquarters Marine Corps Command, Control, Communication, and Computers to ensure the Federal Information Security Management Act tab is updated with accreditation documents as soon as they are completed. Based upon U.S. Marine Corps actions completed, the Marine Corps requests the Naval Audit Service close Recommendation 8.

Naval Audit Service comment on the response to Recommendation 8. Commandant of the Marine Corps actions taken meet the intent of the recommendation. We consider this recommendation closed. In subsequent communication, Commandant of the Marine Corps stated that the actions were taken as of 9 May 2011.

Finding 3: Management Internal Controls

Synopsis

The audit disclosed additional management internal control weaknesses that may potentially undermine the security of the Marine Corps Information Assurance program. These conditions existed because management internal controls were not sufficient to ensure that the information assurance program was fully executed. Specifically, we identified the following weaknesses: (1) omission of the Department of Defense (DoD) reciprocity agreement; (2) unregistered information systems; and (3) outdated Marine Corps guidance. The United States General Accounting Office defines internal control as an integral component of an organization's management that provides reasonable assurance that the following objectives are being achieved: (1) effectiveness and efficiency of operations; (2) reliability of financial reporting; and (3) compliance with applicable laws and regulations. Allowing these internal control weaknesses to persist potentially exposes the Marine Corps and other DoD components to unacceptable levels of risk and may result in the loss of Congressional funding.

Discussion of Details

Background

According to General Accounting Office² Standards for Internal Control in the Federal Government, Federal policymakers are continually seeking ways to better achieve agencies' missions and program results. A key factor in minimizing operational problems and achieving positive outcomes is to implement appropriate internal controls. As agencies strive to improve operational processes and implement new technological developments, management must continually evaluate its internal controls for effectiveness. The Federal Managers' Financial Integrity Act of 1982 requires the General Accounting Office to issue standards for internal controls in Government. The standards provide the overall framework for establishing and maintaining internal controls to reduce the risk of fraud, waste, and mismanagement.

² The General Accounting Office is now the Government Accountability Office; however, the internal control guidance was established prior to the name change.

Audit Results

Omission of the DoD Reciprocity Agreement

Marine Corps Systems Command did not forward certification and accreditation packages to the Designated Accrediting Authority who would establish reciprocity agreements for two Navy-owned information systems in use by the Marine Corps. Consequently, they were not in compliance with the DoD reciprocity agreement. According to the “DoD Information System Certification and Accreditation reciprocity” memorandum, dated 23 July 2009, the receiving DoD component’s Designated Accrediting Authority shall: (1) accept/sanction the originating Designated Accrediting Authority’s accreditation decision; (2) assess and accept the residual risk for the DoD component enclaves receiving the information systems and authorize its connection to the DoD component network; and (3) ensure information assurance controls will not be tested for recertification. Naval Air Systems Command prepared certification and accreditation packages for two information systems that were granted Navy-issued “authority to operate” designations. The certification and accreditation packages were received by the Marine Corps Systems Command. However, the command wanted to complete their own certifications and did not submit the Navy’s certification and accreditation packages to the Designated Accrediting Authority for accreditation designations. Because the certification and accreditation personnel did not submit the comprehensive certification and accreditation packages to the Designated Accrediting Authority as directed in the memorandum, one system lost \$15,000 in Operation and Maintenance funding. Failure to follow the DoD memorandum regarding reciprocity may result in the loss of additional funding for Marine Corps information systems.

Unregistered Information Systems

The Marine Corps did not list 408 (73 percent) of 560 operational information systems in the DoD Information Technology Portfolio Repository-DON. The Marine Corps Systems Command Certifying Authority provided the auditors with a list of 560 documented operating systems. Of the 560 listed, only 152 systems (27 percent) were registered in the DON repository. For the remaining 408, the Certifying Authority could not properly identify the operational status of information systems, and was unable to disclose whether the Marine Corps was the originating component owner of the 408 systems. Additionally, the Marine Corps Systems Command Certifying Authority representative said that certification and accreditation personnel overlooked registering mission support systems in DON repository. The DON repository registration guidance for 2006 “requires registration of all Mission Critical, Mission Essential, and Mission Support information systems.” Also, each originating DoD component is responsible for maintaining the most current and accurate inventory for the information systems they own. Through the review, we determined the Marine Corps did not have management

internal controls in place to perform periodic reviews and effectively monitor operational information systems. Operational systems that are not inventoried or properly managed expose the Marine Corps network to unacceptable levels of risk and potential loss of funding.

Outdated Marine Corps Guidance

Marine Corps Order 5239.2 “Marine Corps Information Assurance Program,” dated 18 November 2002, is outdated and does not include the current DoD Information Assurance Certification and Accreditation Process, which has been in effect since 28 November 2007. Instead, Marine Corps Order 5239.2 describes the DoD Information Technology Security Certification and Accreditation Process, which is no longer in use. In February 2008, Naval Audit Service audit report, “Information Security within the Marine Corps” (N2008-0023), recommended that the Commandant of the Marine Corps review and update Marine Corps Order 5239.2 and related information resource manuals as needed. The Director of Headquarters Marine Corps, Command, Control, Communications, and Computers concurred with the recommendation. The director said, “Headquarters Marine Corps, Command, Control, Communications, and Computers Information Assurance Division will staff and promulgate the update to Marine Corps Order 5239.2 and related Information Resource Manuals no later than January 2009.” To date, the Marine Corps has not revised Marine Corps Order 5239.2 as concurred to in the previous audit report. Additionally, management has a draft version of Marine Corps Order 5239.2A, which includes revisions to ensure compliance with DoD and DON certification and accreditation process guidance; however, the order still has not been signed. Not updating Marine Corps Order 5239.2 to describe the current certification and accreditation process requirements may be one factor contributing to the inconsistencies observed in the Marine Corps certification and accreditation process.

Recommendations and Corrective Actions

Our recommendations, summarized management responses, and our comments on the responses are presented below. The complete text of the management responses is in the Appendix.

We recommend that the Commandant of the Marine Corps:

Recommendation 9. Establish enforcement mechanism(s) to ensure that certification and accreditation command personnel comply with the Department of Defense reciprocity memorandum and directly submit all certification and accreditation packages prepared by other military services to the Designated Accrediting Authority for an accreditation decision.

Commandant of the Marine Corps response to Recommendation 9. Concur, with comments. The Department of Defense Information System Certification and Accreditation reciprocity memorandum calls for certification reciprocity and not accreditation reciprocity. Receiving service Designated Accrediting Authorities' are not required to always accept other service's accreditation decisions since each network under a Designated Accrediting Authority's purview is unique, has its own levels of risk, and operates under its own requirements. What may be acceptable to one network/Designated Accrediting Authority may be extremely risky to another network/Designated Accrediting Authority.

Each received system package needs to be viewed in the context of the network it will operate on. Unless the receiving system is employed in the same manner and on the same type network as the delivering service, then there will be differences in the ways the Information Assurance controls are implemented. For example, the delivering service may inherit a large percentage of their controls from a hosting site while the receiving site may either inherit all or part of those controls from a completely different site or may have to implement some of the controls on their own. Those differences need to be evaluated and potentially tested so that the Designated Accrediting Authority can make an informed risk management decision; hence, the need for system package reviews.

The certification phase is the most costly aspect of certification and accreditation, it has always been policy to use as much documentation from the delivering service as possible to avoid costly duplication and to make a timely and informed accreditation decision while putting the incoming system's risk in its proper operating context. Since the conclusion of the audit, and in preparation for this formal response, we reminded Systems Engineering, Interoperability, Architectures and Technology Division at their Information Assurance Managers bi-monthly meeting (on 24 June 2011) that packages coming to the Marine Corps from outside entities under the reciprocity approach had to come directly to the Designated Accrediting Authority for determination of certification. Based upon U.S. Marine Corps actions completed, the Marine Corps requests the Naval Audit Service close Recommendation 9.

Naval Audit Service comment on the response to Recommendation 9. We requested that the Commandant of the Marine Corps enforce to command personnel to comply with the Department of Defense reciprocity memorandum and directly submit all certification and accreditation packages prepared by other military services to the Designated Accrediting Authority for an accreditation decision. We agree that the Designated Accrediting Authority has the right to accept or decline packages submitted for review. This recommendation is intended to ensure that the Designated Accrediting Authority is aware of all systems submitted through a reciprocity agreement.

The Commandant chose to enforce compliance via their Information Assurance Managers bi-monthly meeting, and will continue to reinforce that all packages must be submitted to the Designated Accrediting Authority for review. Commandant of the Marine Corps actions taken met the intent of the recommendation. We consider this recommendation closed as of 24 June 2011.

Recommendation 10. Establish management oversight to effectively monitor operational information systems, and ensure that all information systems operating on the Marine Corps network are registered in the Department of Defense Information Technology Portfolio Repository-Department of the Navy.

Commandant of the Marine Corps response to Recommendation 10. Concur. The Marine Corps Chief Information Officer Office, in coordination with Marine Corps Systems Command Systems Engineering, Interoperability, Architectures and Technology Division, is currently reviewing the systems both within and outside of Department of Defense Information Technology Portfolio Repository-Department of the Navy. It has been noted that many of the systems are different versions of the same system. The Department of Defense Information Technology Portfolio Repository-Department of the Navy database is limited in functionality and does not differentiate among different variants, which skews reporting and monitoring. Headquarters Marine Corps Command, Control, Communication, and Computers is currently discussing Department of Defense Information Technology Portfolio Repository-Department of the Navy policy and application change requests with the Department of the Navy and Department of Defense Chief Information Officers to address these limitations. The target completion date for corrective actions in response to Recommendation 10 is 15 September 2011.

Naval Audit Service comment on the response to Recommendation 10. Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 11. Require command personnel to validate the status of the 408 information systems and provide assurance that they are registered in the Department of Defense Information Technology Portfolio Repository-Department of the Navy.

Commandant of the Marine Corps response to Recommendation 11. Concur, with comments. The Marine Corps Chief Information Officer Office, in coordination with Marine Corps Systems Command Systems Engineering, Interoperability, Architectures and Technology Division, is currently reviewing the systems both within and outside of Department of Defense Information

Technology Portfolio Repository-Department of the Navy. It has been noted that many of the systems are different versions of the same system. The Department of Defense Information Technology Portfolio Repository-Department of the Navy database is limited in functionality and does not differentiate among different variants, which skews reporting and monitoring. Headquarters Marine Corps Command, Control, Communication, and Computers is currently discussing Department of Defense Information Technology Portfolio Repository-Department of the Navy policy and application change requests with the Department of the Navy and Department of Defense Chief Information Officers to address these limitations. The target completion date for corrective actions in response to Recommendation 11 is 15 September 2011.

Naval Audit Service comment on the response to Recommendation 11.

Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Recommendation 12. Sign and promulgate Marine Corps Order 5239.2A, which includes the current certification and accreditation process (Department of Defense Assurance Certification and Accreditation Process), and ensure that future updates and other requirements adhere to Department of Defense guidance.

Marine Corps response to Recommendation 12. Concur. Marine Corps Order 5239.2A has completed a 12-month staffing within Headquarters Marine Corps and been returned to Command, Control, Communication, and Computers Cybersecurity Division for updates. The order is being updated and will be staffed for final review before signatory routing. The target completion date for corrective actions in response to Recommendation 12 is 15 September 2011.

Naval Audit Service comment on the response to Recommendation 12.

Commandant of the Marine Corps' planned actions meet the intent of the recommendation. We consider this recommendation open pending completion of agreed-to actions.

Section B:

Status of Recommendations

Recommendations							
Finding ³	Rec. No.	Page No.	Subject	Status ⁴	Action Command	Target or Actual Completion Date	Interim Target Completion Date ⁵
1	1	10	Establish controls and governance to ensure that certification and accreditation packages are complete and contain the required Department of Defense Information Assurance Certification and Accreditation Process documentation to support accreditation.	O	Commandant of the Marine Corps	9/1/11	
1	2	11	Establish management internal controls to ensure that information systems have appropriate documentation to support the certifying authority's certification recommendation prior to issuing an accreditation.	O	Commandant of the Marine Corps	9/1/11	
1	3	12	Establish enforcement mechanism(s) to ensure that certified information systems have a formal accreditation letter to document the Designated Accrediting Authority's designation.	O	Commandant of the Marine Corps	9/1/11	
1	4	12	Establish enforcement mechanism(s) to ensure that the oversight process identifies Marine Corps information systems approaching expired accreditation and timely recertification and reaccreditation prior to expiration.	O	Commandant of the Marine Corps	9/1/11	
1	5	12	Establish enforcement mechanism(s) and standard operating procedures to ensure that Marine Corps commands are consistently using Xacta as prescribed by Marine Corps Bulletin 5239.	O	Commandant of the Marine Corps	9/1/11	
1	6	13	Comply with the Department of Defense Information Assurance Certification and Accreditation Process by issuing approved and recognized accreditation designations to Marine Corps information systems.	O	Commandant of the Marine Corps	9/1/11	

³ / + = Indicates repeat finding.

⁴ / O = Recommendation is open with agreed-to corrective actions; C = Recommendation is closed with all action completed; U = Recommendation is undecided with resolution efforts in progress.

⁵ If applicable.

Recommendations							
Finding ³	Rec. No.	Page No.	Subject	Status ⁴	Action Command	Target or Actual Completion Date	Interim Target Completion Date ⁵
1	7	13	Obtain the required documentation for the 44 systems that were given the "limited authority to operate" designation, and ensure that all elements of the Department of Defense Information Assurance Certification and Accreditation Process are met.	O	Commandant of the Marine Corps	9/15/11	
2	8	18	Establish management internal controls to ensure that data elements are completed in compliance with Federal Information Security Management Act reporting standards, are supported, and accurately posted into the Department of Defense Information Technology Portfolio Repository-Department of the Navy.	C	Commandant of the Marine Corps	5/9/11	
3	9	21	Establish enforcement mechanism(s) to ensure that certification and accreditation command personnel comply with the Department of Defense reciprocity memorandum and directly submit all certification and accreditation packages prepared by other military services to the Designated Accrediting Authority for an accreditation decision.	C	Commandant of the Marine Corps	6/24/11	
3	10	23	Establish management oversight to effectively monitor operational information systems, and ensure that all information systems operating on the Marine Corps network are registered in the Department of Defense Information Technology Portfolio Repository-Department of the Navy.	O	Commandant of the Marine Corps	9/15/11	
3	11	23	Require command personnel to validate the status of the 408 information systems and provide assurance that they are registered in the Department of Defense Information Technology Portfolio Repository-Department of the Navy.	O	Commandant of the Marine Corps	9/15/11	
3	12	24	Sign and promulgate Marine Corps Order 5239.2A, which includes the current certification and accreditation process (Department of Defense Assurance Certification and Accreditation Process), and ensure that future updates and other requirements adhere to Department of Defense guidance.	O	Commandant of the Marine Corps	9/15/11	

Background and Pertinent Guidance

Background Information

Information assurance is the cornerstone in providing a secure, interoperable, information management/information technology environment across the Department of the Navy (DON). The confidentiality, integrity, availability, and technical superiority of DON information systems are critical to maintaining our maritime dominance and national security. An integral part of information assurance is the certification and accreditation of information systems. This process ensures that information systems are providing adequate security for data management within the Department of Defense (DoD) and complying with applicable laws and regulations. Certification is the comprehensive evaluation of the technical and non-technical security safeguards of an information system. Accreditation ensures that unacceptable risk is not introduced into operational networks and systems through a formal declaration by an approving authority. The declaration states that an information technology system is compliant with established security requirements and is approved to operate using a prescribed set of standards. The certification and accreditation process has a major impact on the assurance that information systems provide adequate security to minimize environmental risk across the DON enterprise.

Information assurance is an area of focus for DON leadership and external agency reviews. In 2008, Naval Audit Service Report N2008-0023 identified problems with incomplete, missing, or outdated certification and accreditation records at 7 of 10 activities visited. The Government Accountability Office-07-528 audit report stated that the DoD Inspector General rated DoD's certification and accreditation process as "poor."

Because information assurance is critical for national security, the Federal Government has endeavored to improve it through strengthening internal controls and standardizing procedures. The Federal Information Security Management Act permanently authorized and strengthened the information security program, evaluation, and reporting requirements established by the Government Information Security Reform Act. The Federal Information Security Management Act mandates that all agencies test and evaluate the effectiveness of information security, policies, procedures, and practices at least annually.

The implementation of the DoD Information Assurance Certification and Accreditation Process works to create standardization across the entire DoD. Issued on 28 November 2007, the certification and accreditation process evaluates information assurance principles and controls to ensure that they provide adequate protection for our

information assets. As the overarching certification and accreditation process for the DoD, the certification and accreditation process validates security requirements, examines implemented safeguards, and identifies any inadequacies.

Implementation of the certification and accreditation process will allow the Marine Corps to comply with DoD policy and result in a standardized certification and accreditation program. Proper use of the certification and accreditation methodology will assure Marine Corps leadership that an appropriate level of security is implemented, sufficient controls are in place to adequately protect assets, and information systems are operating at an acceptable level of residual risk. Marine Corps implementation of the process: provides visibility into the implementation of information assurance capabilities and services throughout the certification and accreditation process; facilitates collaboration among the stakeholders; and speeds the decision to authorize the operation of a given information system.

The DoD Information Assurance Certification and Accreditation Process is applicable to all commands, bases, ships, organizations, and units that own and operate information systems within DON. The certification and accreditation process ensures that adequate security measures are in place to protect the information that resides on DON networks. This process is applicable to all DON systems under development and those already in production. The Navy and Marine Corps may provide service-unique amplification to successfully execute these procedures while maintaining the intent of certification and accreditation process. In July 2008, the Navy and Marine Corps Designated Accrediting Authorities jointly issued the DON DoD Information Assurance Certification and Accreditation Process Handbook.

Certification is the comprehensive evaluation of the technical and non-technical security safeguards of an information system. The Certifying Authority performs a comprehensive evaluation and validation of a DoD information system, establishing the degree to which it complies with assigned information assurance controls. These controls are standardized procedures that include an examination of threats to the system and the data that resides on it. Additionally, the Certifying Authority evaluates the security functions (i.e., technical features) of an information system and the assurance that those functions are correctly implemented. Once the Certifying Authority is satisfied with the residual risk involved in operating the system, this authority will issue a statement regarding a system's compliance with information assurance controls. A certification statement from the Certifying Authority is submitted to the Designated Accrediting Authority for an accreditation decision. In order for a system to be operationally deployed, it must receive an accreditation approval from the Designated Accrediting Authority.

Accreditation is the formal declaration by the Designated Accrediting Authority that an information system is compliant with established security requirements and is approved

to operate using a prescribed set of safeguards. Accreditation minimizes unacceptable risks to operational networks and systems. The Designated Accrediting Authority issues an accreditation decision for the information system based upon the certification statement provided by the Certifying Authority, along with an impact assessment of the Global Information Grid. In addition to the specific information provided by the Certifying Authority, the Designated Accrediting Authority takes into consideration Marine Corps missions, current threat levels, and the overarching security posture of the Global Information Grid.

Pertinent Guidance

Office of Management and Budget Circular A-130, “Management of Federal Information Resources,” dated December 1985

Circular A-130 was first issued in December of 1985 to meet information resource management requirements that were included in the Paperwork Reduction Act of 1980. Specifically, the Act assigned responsibility to the Office of Management and Budget Director to develop and maintain a comprehensive set of information resources management policies for use across the Federal Government. It also required the director to promote the application of information technology to improve the use and dissemination of information in the operation of Federal programs.

Federal Information Security Management Act of 2002, dated December 2002

In 2002, the Federal Information Security Management Act recognized the importance of information security to the economic and national security interests of the United States. The act requires each Federal agency to develop, document, and implement an agency-wide program to provide security for information systems that support the operations and assets of the agency. The Act requires agency program officials, chief information officers, and inspectors general to conduct annual reviews of agencies’ information security programs and report the results to the Office of Management and Budget. The Office of Management and Budget uses this data to assist in its oversight responsibilities and prepare an annual report to Congress on agency compliance with the act.

DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” dated February 2003

This instruction provides an overview of the DoD Information Assurance program, which implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of DoD information systems and networks. The instruction also lays out the multi-tiered management structure and information standards used for assessing, implementing, verifying, and managing changes to information assurance needs and capabilities.

DoD Instruction 8510.01, “DoD Information Assurance Certification and Accreditation Process,” dated 28 November 2007

This instruction establishes a certification and accreditation process to manage the implementation of information assurance controls and provides visibility of accreditation decisions regarding the operation of DoD Information Systems. It also prescribes the certification and accreditation process to satisfy the requirements of the security management Act.

DoD Information Technology Portfolio Repository - Department of the Navy Registration Guidance for 2006, dated June 2006

This guide is intended to provide program managers, system owners, command information officers, functional area managers and others with specific guidance for registering information technology systems, including national security systems, in the DoD Information Technology Portfolio Repository- Department of the Navy and updating data already in that repository.

DoD Information System Certification and Accreditation Reciprocity memorandum, dated July 2009

Reciprocity of accreditation decisions and the artifacts contributing to the accreditation decision will advance information sharing and reduce rework and cycle time when establishing information systems to support DoD mission accomplishment. This memorandum implements the security terms and conditions for certification and accreditation reciprocity in accordance with published DoD guidance.

Secretary of the Navy Instruction 5239.3B, “Department Of The Navy Information Assurance Policy,” dated June 2009

This instruction requires registration of all DON information systems or networks that meet the qualification for registration in the DoD Information Technology Portfolio Repository. Registration in the repository is accomplished by registration in the DON variant of the repository, according to Secretary of the Navy Instructions 5000.2D and 5000.36A, as well as the DON repository guidance issued by the Department of the Navy Chief Information Officer.

Secretary of the Navy Manual 5239.1, “Information Assurance Manual,” dated November 2005

This manual is intended to serve as a high-level introduction to information assurance and its principles. It discusses common information assurance controls and associated requirements and reviews the Department of Defense strategy for implementing those controls.

DON DoD Information Assurance Certification and Accreditation Process Handbook, dated July 2008

This handbook defines the DON approach to implementing certification and accreditation process procedures and documentation. Further, it identifies the roles and responsibilities of key players, explains the different types of certification and accreditation recommendations and decisions, and describes the activities and process steps that comprise the certification and accreditation process.

DON Chief Information Officer Message, “Certification of Compliance with Information Technology Systems Registration,” dated August 2009

This Naval message directs all DON mission critical, mission essential and mission support information technology systems, including national security systems, to be registered in the DON repository.

Marine Corps Bulletin 5239, “USMC [United States Marine Corps] Certification and Accreditation Program,” dated March 2009

This Marine Corps bulletin announces policy related to the certification and accreditation of Marine Corps information systems. Specifically, it designates the Xacta Information Assurance Manager Assessment Engine as the tool that commands will use to accomplish certification and accreditation efforts for Marine Corps information systems.

Exhibit B:

Scope and Methodology

Scope

Our audit reviewed the internal controls for the certification and accreditation process within the Marine Corps to verify that information systems were certified, accredited, and maintained in accordance with Department of Defense (DoD) Information Assurance Certification and Accreditation Process, and whether activities were in compliance with the Federal Information Security Management Act reporting standards. Specifically, we assessed whether Marine Corps: (1) information systems fulfilled certification and accreditation process requirements; and (2) commands accurately reported security management Act data elements for Congressional review.

Our audit work began 25 May 2010 and was completed 17 March 2011. We obtained and reviewed documentation related to certification, accreditation, and security management Act reporting requirements within the Marine Corps. We judgmentally selected 60 systems from the 152 Marine Corps information systems listed in the DoD Information Technology Portfolio Repository- Department of the Navy. We did not test the reliability of this system because it was outside the scope of this audit. The review was conducted at two Marine Corps locations: Headquarters Marine Corps, VA and Marine Corps Base Quantico, VA. We also interviewed personnel representing roles needed to accomplish the certification and accreditation. For a list of the activities visited or contacted, see Exhibit C.

Methodology

We conducted this audit in accordance with Generally Accepted Government Auditing Standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

To accomplish our audit, we used data from the DON repository to select activities and information systems for auditing. As of 12 May 2010, there were 152 information systems listed in the DON repository. Those systems were owned and maintained by one of four Marine Corps commands. A 100-percent review was performed for the three commands with 15 or fewer information systems (13 systems from Marine Corps Logistics Command, GA; 11 systems from Headquarters Marine Corps, VA; and

8 systems from Marine Corps Community Services, VA). For the fourth command (Marine Corps Systems Command, VA), we reviewed 28 of their 92 information systems of record. We selected 9 of the 28 because their accreditation was expired, and for the remaining 19, we made an arbitrary selection, resulting in a final total sample of 60 information systems spread across all 4 commands.

We judgmentally selected these 60 information systems as described above, to determine if they were properly certified and accredited. In addition, we reviewed documentation to ascertain whether the information systems were in compliance with security management Act reporting requirements. We made inquiries and held discussions with key certification and accreditation personnel at the activities contacted or visited. We obtained and examined pertinent documentation, records, reports, and reviewed procedures used. We evaluated compliance with legal and regulatory requirements, and assessed internal controls related to certification, accreditation, and Federal Information Security Management Act within the Marine Corps by reviewing certification and accreditation documentation, and interviewing personnel overseeing the Marine Corps information systems. Additionally, we followed up on Naval Audit Service audit report, “Information Security within the Marine Corps” (N2008-0023) to check corrective action on Certification and Accreditation issues cited.

Exhibit C:

Activities Visited and/or Contacted

Arlington, VA

- Department of Navy Chief Information Officer*
- Headquarters United States Marine Corps*
- Headquarters Marine Corps, Command, Control, Communications and Computers-Information Assurance*

Quantico, VA

- Marine Corps Community Services
- Marine Corps Systems Command*
- Marine Corps Network Operations and Security Command*
- Marine Corps Base Quantico*

Virginia Beach, VA

- Naval Network Warfare Command

Albany, GA

- Marine Corps Logistics Command
- Marine Corps Logistics Base Albany

Oceanside, CA

- Marine Corps Base Camp Pendleton

Cherry Point, NC

- Marine Corps Air Station Cherry Point

Jacksonville, NC

- Marine Corps Base Camp Lejeune

Halawa, HI

- Camp H.M. Smith
- Marine Forces Pacific

* Activities Visited

Appendix:

Management Response from Commandant of the Marine Corps



DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350-3000

IN REPLY REFER TO:
7510
REF-80
JUN 28 2011

From: Commandant of the Marine Corps
To: Assistant Auditor General for Financial Management and
Comptroller Audits, Naval Audit Service

Subj: COMMANDANT OF THE MARINE CORPS (CMC) OFFICIAL RESPONSE
TO NAVAL AUDIT SERVICE (NAVAUDSVC) DRAFT REPORT
N2010-NFA000-0101, "CERTIFICATION AND ACCREDITATION OF
INFORMATION SYSTEMS WITHIN THE MARINE CORPS," DATED
17 MARCH 2011

Ref: (a) NAVAUDSVC memo 7510 N2010-NFA000-0101 17 Mar 2011

Encl: (1) CMC Official Responses

1. Official responses required by the reference are provided at the enclosure.
2. Enclosure (1) was coordinated with Headquarters, U. S. Marine Corps, Programs and Resources; and Command, Control, Communications, and Computers (C4).
3. The Marine Corps appreciates the opportunity to respond to the report.
4. If you have any questions about the responses, please contact [REDACTED] Headquarters, U. S. Marine Corps Senior Audit Liaison, email [REDACTED] or phone [REDACTED]

FOIA (b)(6)

[REDACTED]
[REDACTED]
Deputy Commandant
for Programs and Resources

FOIA (b)(6)

Copy to:
NAVINGEN (N4)
DMCS
Dir C4

NAVAL AUDIT SERVICE (NAS) DRAFT REPORT # N2010-NFA000-0101
DATED 17 MARCH 2011 - PROJECT # N2010-NFA000-0101

"CERTIFICATION AND ACCREDITATION OF INFORMATION SYSTEMS
WITHIN THE MARINE CORPS"

COMMANDANT OF THE MARINE CORPS RESPONSES
TO THE NAS RECOMMENDATIONS

RECOMMENDATION 1: NAS recommends that the Commandant of the Marine Corps establish controls and governance to ensure that certification and accreditation packages are complete and contain the required Department of Defense Information Assurance Certification and Accreditation Process documentation to support accreditation.

CMC RESPONSE: Concur. The Marine Corps had established controls and governance in place at the time of the audit, e.g., Enterprise Information Assurance (IA) Directive 018 - Marine Corps Certification & Accreditation Process, as well as numerous MARADMIN messages; however, there was no process in place to validate and enforce policies or to implement appropriate consequences for instances when compliance was not found. The Marine Corps will update Enterprise IA Directive 018 with specific requirements, responsibilities, and standards - including specific consequences for compliance failure. The directive is currently in staffing and will be coordinated, then presented at the next Marine Corps Cybersecurity Conference by 5 August 2011. A final version will be signed by the Director, C4 by 1 September 2011; the target completion date for corrective actions in response to recommendation 1 is 1 September 2011.

RECOMMENDATION 2: NAS recommends that the Commandant of the Marine Corps establish management internal controls to ensure that information systems have appropriate documentation to support the certifying authority's certification recommendation prior to issuing an accreditation.

CMC RESPONSE: Concur. The Marine Corps had controls in place to require documentation and certification authority recommendations for accreditation; however, there are other certification authority representatives throughout the Marine Corps, e.g., G-6 officers at base, posts, and stations, who can also provide recommendations for

accreditation. The Senior IA Official (SIAO), as noted in DoDI 8510.01 - DoD IA C&A Process (DIACAP), is the service certification authority. According to the DIACAP, the SIAO can also function as the accrediting official (DAA). This is the case with the Marine Corps. Some certification authority responsibility was delegated to the Technical Director at Marine Corps Systems Command (MCSC); however, there were times when mission expediency, combined with independent scans and assessments, were sufficient to make an accreditation decision. The current re-write to Enterprise IA Directive 018 will ensure that documentation from the delegated certifying authority and the distributed certification authority representatives is standardized through the use of the current automated Certification and Accreditation (C&A) document repository in the Telos Xacta automated tool. The Enterprise IA Directive 018 will be finalized and signed by the Director, C4 by 1 September 2011; the target completion date for corrective actions in response to recommendation 2 is 1 September 2011.

RECOMMENDATION 3: NAS recommends that the Commandant of the Marine Corps establish enforcement mechanism(s) to ensure that certified information systems have a formal accreditation letter to document the Designated Accrediting Authority's designation.

CMC RESPONSE: Concur. The mandated use of the Telos Xacta automated tool ensures all information systems in the Marine Corps have an audit trail of appointments, recommendations, and approvals. All instances of alternate documentation procedures have been directed to be halted and accreditation actions to be accomplished in the automated tool. This will be included in the Enterprise IA Directive 018, estimated to be signed by the Director, C4 by 1 September 2011; the target completion date for corrective actions in response to recommendation 3 is 1 September 2011.

RECOMMENDATION 4: NAS recommends that the Commandant of the Marine Corps establish enforcement mechanism(s) to ensure that the oversight process identifies Marine Corps information systems approaching expired accreditation and timely recertification and reaccreditation prior to expiration.

CMC RESPONSE: Concur. Enterprise IA Directive 018 will include timeline requirements for scheduled reviews based on expiration dates vice arbitrary schedules. The metric of

success will be measured by the Federal Information Security Management Act quarterly and annual approval-to-operate scores. The process and documentation will be tracked in the Telos Xacta automated tool. The Enterprise IA Directive 018 will be finalized and signed by the Director, C4 by 1 September 2011; the target completion date for corrective actions in response to recommendation 4 is 1 September 2011.

RECOMMENDATION 5: NAS recommends that the Commandant of the Marine Corps establish enforcement mechanism(s) and standard operating procedures to ensure that Marine Corps commands are consistently using Xacta as prescribed by Marine Corps Bulletin 5239.

CMC RESPONSE: Concur. Enterprise IA Directive 018 will codify the mandatory use of the Telos Xacta automated tool by including the wording from the MCBUL and previous MARADMINS on the topic. At present, no other documentation process, e.g., Information Assurance Control Implementation Determination (IACID), is authorized or being used to accredit Marine Corps systems. The Enterprise IA Directive 018 will be finalized and signed by the Director, C4 by 1 September 2011; the target completion date for corrective actions in response to recommendation 5 is 1 September 2011.

RECOMMENDATION 6: NAS recommends that the Commandant of the Marine Corps comply with the Department of Defense Information Assurance Certification and Accreditation Process by issuing approved and recognized accreditation designations to Marine Corps information systems.

CMC RESPONSE: Concur. All accreditation documentation [reviewed during the audit] was in accordance with DON and DoD policy. The Designated Accrediting Authority (DAA) has always been authorized to outline restrictions, limitations, and conditions of accreditation, to ensure the systems owners and program managers understand the boundaries and requirements to operate securely and with an acceptable level of risk. Titles/designations will be standardized to prevent confusion for anyone not familiar with the C&A process, and to ensure consistent tracking of accreditation documentation. Approved and recognized accreditation designations will be included in the Enterprise IA Directive 018, estimated to be signed by the Director, C4 by 1 September 2011; the target completion date for corrective actions in response to recommendation 6 is 1 September 2011.

RECOMMENDATION 7: NAS recommends that the Commandant of the Marine Corps obtain the required documentation for the 44 systems that were given the "limited authority to operate" designation, and ensure that all elements of the Department of Defense Information Assurance Certification and Accreditation Process are met.

CMC RESPONSE: Concur. All accreditation documentation [reviewed during the audit] was in accordance with DON and DoD policy. The DAA has always been authorized to outline restrictions, limitations, and conditions of accreditation, to ensure the systems owners and program managers understand the boundaries and requirements to operate securely and with an acceptable level of risk. Titles/designations will be standardized to prevent confusion for anyone not familiar with the C&A process, and to ensure consistent tracking of accreditation documentation. This will be included in the Enterprise IA Directive 018, estimated to be signed by the Director, C4 by 1 September 2011. The particular systems in question by this audit have been issued Denial of Approval to Operate (DATO) memos, and are now in the process of going through the reaccreditation process through Xacta. Systems will be re-accredited by 15 September 2011 or they will continue to be under the DATO and disconnected. The target completion date for corrective actions in response to recommendation 7 is 15 September 2011.

RECOMMENDATION 8: NAS recommends that the Commandant of the Marine Corps establish management internal controls to ensure that data elements are completed in compliance with Federal Information Security Management Act reporting standards, are supported, and accurately posted into the Department of Defense Information Technology Portfolio Repository-Department of the Navy.

CMC RESPONSE: Concur. The newly created HQMC C4 Chief Information Officer Division supports the Marine Corps CIO with maintaining and supervising DITPR-DON policy. HQMC C4 Cybersecurity Division has the responsibility to ensure the Federal Information Security Management Act (FISMA) tab to DITPR-DON is updated with appropriate artifacts in a timely manner. Policies have been implemented by HQMC C4 to ensure the FISMA tab is updated with accreditation documents as soon as they are completed. Based upon USMC actions completed, the Marine Corps requests NAS close recommendation 8.

RECOMMENDATION 9: NAS recommends that the Commandant of the Marine Corps establish enforcement mechanism(s) to ensure that certification and accreditation command personnel comply with the Department of Defense reciprocity memorandum and directly submit all certification and accreditation packages prepared by other military services to the Designated Accrediting Authority for an accreditation decision.

CMC RESPONSE: Concur, with comments. The DoD Information System Certification and Accreditation reciprocity memorandum calls for certification reciprocity and not accreditation reciprocity. Receiving service DAA's are not required to always accept other service's accreditation decisions since each network under a DAA's purview is unique, has its own levels of risk, and operates under its own requirements. What may be acceptable to one network/DAA may be extremely risky to another network/DAA.

Each received system package needs to be viewed in the context of the network it will operate on. Unless the receiving system is employed in the same manner and on the same type network as the delivering service, then there will be differences in the ways the IA controls are implemented. For example, the delivering service may inherit a large percentage of their controls from a hosting site while the receiving site may either inherit all or part of those controls from a completely different site or may have to implement some of the controls on their own. Those differences need to be evaluated and potentially tested so that the DAA can make an informed risk management decision; hence, the need for system package reviews.

Since the certification phase is the most costly aspect of certification and accreditation, it has always been policy to use as much documentation from the delivering service as possible to avoid costly duplication and to make a timely and informed accreditation decision while putting the incoming system's risk in its proper operating context. Based upon USMC actions completed, the Marine Corps requests NAS close recommendation 9.

RECOMMENDATION 10: NAS recommends that the Commandant of the Marine Corps establish management oversight to effectively monitor operational information systems, and ensure that all information systems operating on the Marine Corps network are registered in the Department of Defense

Information Technology Portfolio Repository-Department of the Navy.

CMC RESPONSE: Concur. The Marine Corps CIO Office in coordination with Marine Corps Systems Command SIAT Division is currently reviewing the systems both within and outside of DITPR-DON. It has been noted that many of the systems are different versions of the same system. The DITPR-DON database is limited in functionality and does not differentiate among different variants which skew reporting and monitoring. HQMC C4 is currently discussing DITPR-DON policy and application change requests with the DON CIO and DoD CIO to address these limitations. The target completion date for corrective actions in response to recommendation 10 is 15 September 2011.

RECOMMENDATION 11: NAS recommends that the Commandant of the Marine Corps require command personnel to validate the status of the 408 information systems and provide assurance that they are registered in the Department of Defense Information Technology Portfolio Repository-Department of the Navy.

CMC RESPONSE: Concur, with comments. The Marine Corps CIO Office in coordination with Marine Corps Systems Command SIAT Division is currently reviewing the systems both within and outside of DITPR-DON. It has been noted that many of the systems are different versions of the same system. The DITPR-DON database is limited in functionality and does not differentiate among different variants which skew reporting and monitoring. HQMC C4 is currently discussing DITPR-DON policy and application change requests with the DON CIO and DoD CIO to address these limitations. The target completion date for corrective actions in response to recommendation 11 is 15 September 2011.

RECOMMENDATION 12: NAS recommends that the Commandant of the Marine Corps sign and promulgate Marine Corps Order 5239.2A, which includes the current certification and accreditation process (Department of Defense Assurance Certification and Accreditation Process), and ensure that future updates and other requirements adhere to Department of Defense guidance.

CMC RESPONSE: Concur. MCO 5239.2A has completed a 12-month staffing within HQMC and been returned to C4 Cybersecurity Division for updates. The order is being updated and will be staffed for final review before signatory routing. The target completion date for corrective actions in response to recommendation 12 is 15 September 2011.

ADDITIONAL TECHNICAL COMMENTS: With respect to the comments on page 9 and 10 of the draft report, which stated the DAA was not able to provide documentation to show testing of information assurance controls, the Marine Corps completes monthly security scans for all systems that is accomplished by the regional "Blue Teams", as well as web-site scans by the Marine Corps Web Risk Assessment Cell. Reports are in a repository and are made available covering at least the last two years, and each report shows analysis regarding Information Assurance Vulnerability Alert (IAVA) implementation and security configuration using the DoD mandated security vulnerability analysis tool, eEye Retina. In addition to the Blue Team scans, the Marine Corps Network Operations and Security Center (MCNOSC) sends scanning and security reports to the Joint Task Force-Global Network Operations (JTF-GNO)¹, which are available for review on their portal. Between these two additional sources, the DAA can and has been able to make a risk-based decision regarding the security operations within the Marine Corps enterprise. While any internal inconsistencies will be of continued concern and will continue to be aggressively targeted for remediation, it remains that "risk known" is better than "risk not known." While the Marine Corps will continue to ensure that documented certification recommendations are provided, the DAA had and continues to have sufficient information to accept risk and approve systems for operations, even in the few cases where there may be little to no documented certification recommendations.

¹ Now a part of US Cyber Command

~~FOR OFFICIAL USE ONLY~~

Use this page as

BACK COVER

for printed copies

of this document

~~FOR OFFICIAL USE ONLY~~