Naval Audit Service

Auditor General
Advisory

Risk Assessment of the Department of the Navy Base Realignment and Closure 2005 Information Transfer System

N2005-0042
25 April 2005

Obtaining Additional Copies

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

Phone: (202) 433-5726 (DSN 288)
Fax: (202) 433-5880
Email: 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) 433-5706 (DSN 288)
Fax: (202) 433-5879
Email: 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://www.hq.navy.mil/navalaudit/

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

7510
N2004-NIA300-0042.000
25 Apr 05

MEMORANDUM FOR DEPUTY ASSISTANT SECRETARY OF THE NAVY FOR
INFRASTRUCTURE STRATEGY AND ANALYSIS

Subj: **RISK ASSESSMENT OF THE DEPARTMENT OF THE NAVY BASE REALIGNMENT AND CLOSURE 2005 INFORMATION TRANSFER SYSTEM (AUDITOR GENERAL ADVISORY N2005-0042)**

Ref: (a) NAVAUDSVC memo 7540 N2004-NIA300-0042.000, dated 8 Oct 03
(b) SECNAV memo "Internal Control Plan for Management of the Department of the Navy 2005 Base Realignment and Closure Process Policy Advisory Two," dated 27 Jun 03
(c) SECNAVNOTE 11000, "Base Closure and Realignment," dated 9 Mar 04

1. In accordance with references (a) through (c), the Naval Audit Service completed a risk assessment to measure information technology security assurance for the Department of Navy Base Realignment and Closure (BRAC) 2005 Information Transfer System (DONBITS) developed under contract for the Deputy Assistant Secretary of the Navy for Infrastructure Strategy and Analysis. This advisory provides the results of the risk assessment.

2. Our risk assessment indicates that sufficient management, operational, and technical controls are in place and working as intended to conclude that there is a low overall risk of unauthorized access to DONBITS or manipulation or destruction of electronic data within DONBITS. The Infrastructure Analysis Team and the DONBITS contractor took actions during our review that were based on our suggestions to mitigate risk. The actions reduced our opinion of the overall risk rating to low; therefore, this advisory does not contain any recommendations and does not require a response.

3. We appreciate the cooperation and courtesies extended to our auditors by all those associated with the development and implementation of DONBITS.

Joan T. Hughes

JOAN T. HUGHES
Assistant Auditor General
Installations and Environment Audits

Table of Contents

Executive Summary

Overview

This Auditor General Advisory contains summary information regarding the results of our risk assessment of the Department of the Navy (DON) Base Realignment and Closure (BRAC) 2005 Information Transfer System (DONBITS). During this risk assessment, we reviewed and evaluated the managerial, operational, and technical security measures implemented by the Infrastructure Analysis Team (IAT) and the contractor that developed DONBITS to protect DONBITS and the data it stores.

DONBITS is a web-based data and file collection and management system that facilitates the efficient review of missions and activities/installations by DON during the BRAC 2005 process. DONBITS is the sole and authoritative DON database upon which BRAC recommendations will be made. The DONBITS database will contain all certified data and information pertaining to all DON military activities/installations subject to the Defense Base Closure and Realignment Act of 1990, as amended by the Fiscal Year 2002 National Defense Authorization Act.

The objective of this assessment was to rate the risks associated with the information technology security assurance for DONBITS, provide feedback to lower the risk, evaluate corrective actions taken by IAT and the DONBITS contractor to reduce the risk, and re-evaluate the level of risk. For this advisory, information technology security assurance is defined as the degree of confidence one has that the managerial, operational and technical security measures work as intended to protect DONBITS from unauthorized access and manipulation or destruction of electronic data within DONBITS.

We assessed the managerial, operational, and technical security measures to determine if they are working as intended to protect DONBITS and the data it stores. We used the National Institute of Standards and Technology (NIST) Special Publication 800-26[1] as the criteria to evaluate whether the security measures in place are adequate to protect DONBITS and its data. We used the NIST Special Publication 800-26 Self-Assessment Guide questionnaire that contains specific control objectives and techniques to test and measure the security effectiveness of DONBITS. We completed the questionnaire during October 2003 through 28 October 2004.

[1] NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," dated November 2001.

Objective

The objective of this assessment was to rate the risks associated with the information technology security assurance for DONBITS, provide feedback to lower the risk, evaluate corrective actions taken by IAT and the DONBITS contractor to reduce the risk, and re-evaluate the level of risk. For this advisory, information technology security assurance is defined as the degree of confidence one has that the managerial, operational and technical security measures work as intended to protect DONBITS from unauthorized access and manipulation or destruction of electronic data within DONBITS.

Conclusions

In answering the questionnaire, we evaluated and rated the level of risk of unauthorized access, manipulation, or destruction of electronic data within DONBITS as high, medium, or low. We provided an interim status briefing on 18 December 2003 to the Deputy Assistant Secretary of the Navy for Infrastructure Strategy and Analysis (DASN (IS&A)) showing that we rated 5 of 17 topic areas as highly vulnerable and 12 of 17 as having medium vulnerability, which resulted in a high-risk rating to the Management and Operational and a medium-risk rating to the Technical major control areas. The nature of the issues that caused the high- and medium-risk ratings were primarily related to documentation of the system and controls. Many of the documents provided to the auditors were marked "Draft." Since controls were in place and being executed in accordance with the draft documents, this was more of a technical administrative issue that did not render the system vulnerable to compromise. At the briefing, we identified corrective actions that could be taken to mitigate these risks, which frequently related to finalizing the aforementioned documents. The DASN (IS&A) accepted the level of risk and continued with the deployment of DONBITS. We continually provided feedback and monitored corrective actions taken by IAT and the DONBITS contractor to lower the level of risk and nothing came to our attention to indicate that the DONBITS or its data were vulnerable to unauthorized access or data manipulation. During the period from 18 December 2003 to 28 October 2004, IAT and the DONBITS contractor took suggested actions necessary to reduce to “low” the overall level of risk to the security of DONBITS and the data contained therein. As a result of the final rating of “low” to the overall level of risk to the security of DONBITS and its stored data, we make no recommendations in this advisory.

Section A:

Results of Our Review

Results

The Department of the Navy (DON) Base Realignment and Closure (BRAC) 2005 Information Transfer System (DONBITS) and its data have a high value because data must remain confidential, must be authentic, must be verifiable by a third party, must hold entities submitting data accountable, and the data must be available on a timely basis to meet the requirements of the BRAC 2005 process. DONBITS was rated in both the System Security Plan (SSP) and System Security Authorization Agreement (SSAA) as being a Mission Critical system in support of the Deputy Assistant Secretary of the Navy for Infrastructure Strategy and Analysis (DASN (IS&A)) to distribute/collect official data for the BRAC 2005 process.

Our risk assessment indicates that sufficient management, operational, and technical controls are in place to conclude that there is a low overall risk of unauthorized access, manipulation, or destruction of electronic data within DONBITS.

Our status briefing to the DASN (IS&A) on 18 December 2003 showed that we rated 5 of 17 topic areas as highly vulnerable and 12 of 17 as having medium vulnerability, which resulted in high-risk rating to the Management and Operational and a medium-risk rating to the Technical major control areas. At the briefing, we made suggestions for corrective actions to mitigate these initially determined risks. During the period from the 18 December 2003 status briefing until 28 October 2004, the date we finished our field work, we followed up with responsible DON personnel and support contractors, reviewed the corrective actions taken in response to our preliminary feedback, and adjusted our risk assessment results accordingly. Currently, the Management, Operational, and Technical control areas and 16 of the 17 topic areas are rated as having a low vulnerability to unauthorized access to, or manipulation or destruction of, electronic data within DONBITS as outlined in Figure 1.

Figure 1. Rating of Management, Operational, and Technical control areas by topic area.

Risk Control Area	Level of Risk
Management Controls	**LOW**
Risk Management	LOW
Review of Security Controls	LOW
Life Cycle	LOW
Authorize Processing	LOW
System Security Plan	LOW
Operational Controls	**LOW**
Personnel Security	LOW
Physical and Environmental Protection	LOW
Production, Input/Output Controls	LOW
Contingency Planning	MEDIUM
Hardware and System Software Maintenance	LOW
Data Integrity	LOW
Documentation	LOW
Security Awareness, Training, and Education	LOW
Incident Response Capability	LOW
Technical Controls	**LOW**
Identification and Authentication	LOW
Logical Access Controls	LOW
Audit Trails	LOW

As shown in Figure 1, we found that sufficient management, operational, and technical controls are in place within DONBITS. While the management, operational and technical controls had overall low risk, we concluded that Contingency Planning, one of the nine topic areas within the operational controls risk area, had medium risk.

Corrective Actions

IAT and the DONBITS contractor implemented corrective actions throughout our risk assessment. We tested the adequacy of the corrective actions taken to mitigate the risks that we previously identified, and have subsequently reduced the overall risk rating for unauthorized access to, manipulation of, or destruction of DONBITS and the electronic data within the system to “low;” therefore, there are no recommendations with this advisory.

Exhibit A:

Background

The Defense Base Closure and Realignment Act of 1990, as amended by the Fiscal Year 2002 National Defense Authorization Act, established a process to assess the military infrastructure for timely base closures and realignments. To facilitate this process, the Deputy Assistant Secretary of the Navy for Infrastructure Strategy and Analysis (DASN (IS&A)) awarded a contract in August 2003 for the designing, building, testing, implementation, and management of a web-based system to distribute and collect official data for the Department of the Navy (DON) Base Realignment and Closure (BRAC) 2005 process. The Infrastructure Analysis Team (IAT) [2] was responsible for controlling the development of the DON BRAC 2005 Information Transfer System (DONBITS).

DONBITS is the sole and authoritative DON database upon which BRAC recommendations will be made. The DONBITS database will contain all certified data and information pertaining to all DON military activities/installations subject to the National Defense Authorization Act. DONBITS began issuing questions for the Capacity Data Call on 7 January 2004 to activities subject to the act. DONBITS has continued to collect data call responses and issue subsequent data call questions to more than 800 DON activities.

The acquisition, operation, and sustainment of any Department of Defense (DoD) Information System that collects, stores, transmits, or processes unclassified or classified information must be certified and accredited in accordance with the DoD Information Technology Security Certification and Accreditation Process (DITSCAP). However, the Assistant Secretary of Defense for Networks and Information Integration stated that “contractor information technology systems developed to support Joint Cross Service Groups and other DoD BRAC activities do not constitute a ‘DoD Information System,’ therefore, DITSCAP does not apply.” Since DONBITS is a contractor information technology system developed as a short-term system to solely support DON’s BRAC 2005 activities, DITSCAP’s requirement to obtain full certification and accreditation does not apply to DONBITS.

As part of the DASN (IS&A)’s internal control plan the Naval Audit Service was requested to perform an information technology security assessment of DONBITS to determine if the system and its data are adequately secured. Specifically, the DASN (IS&A) asked the Naval Audit Service to assure that systems and applications operate effectively and provide appropriate confidentiality, integrity,

[2] IAT supports the DASN (IS&A) and controls the development of DONBITS and the associated documentation, and protects the integrity of the process by ensuring that all data, considerations, and evaluations are treated as sensitive and internal to the process.

and availability and protect information commensurate with the level of risk and magnitude of harm resulting from loss, misuse, unauthorized access, or modification. We agreed to perform an assessment of DONBITS using the National Institute of Standards and Technology (NIST) Special Publication 800-26,[3] rate the areas of the assessment as "high," "medium," or "low" risk, and provide suggestions to mitigate the weaknesses found during the assessment.

[3] NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," dated November 2001.

Exhibit B:

Scope and Methodology

The risk assessment was conducted from October 2003 to 28 October 2004.

We determined the significance for DONBITS and the information being assessed using the five protection categories in section 3534(a)(1)(A) of the Government Information Security Reform provisions of the National Defense Authorization Act of 2000 – i.e., integrity, confidentiality, availability, authenticity, and non-repudiation.

We used the answers for selected, pertinent questions contained in NIST Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems," Appendix A, System Questionnaire, to:

- Assess the adequacy of internal controls over the DONBITS;
- Rate the level of risk associated with the control areas;
- Make suggestions to mitigate the risk; and
- Re-evaluate the level of risk after corrective actions were taken.

The NIST System Questionnaire, as amended, consisted of 191 control objective questions covering 17 topics across the 3 major control areas. Each topic contained critical elements and supporting security control objectives and techniques (questions) about the system.

To answer the questions in the NIST System Questionnaire and rate the risk control areas:

- We interviewed DON personnel, to include IAT's System Manager and the Information System Security Officer, the Headquarters Marine Corps Data Center's Head of Configuration Management Section, and DONBITS support contractors.
- We conducted site visits to DON and contractor facilities throughout the risk assessment.
- We analyzed supporting documentation including the:
    - Interim Authority to Operate;
    - Memorandum of Agreement between DONBITS, the Marine Corps Network Operations and Security Command, and the

Headquarters, Marine Corps (HQMC) Administration, and Resources Division, Information Systems Management Branch, HQMC Information Technology Center;

  - System Security Plan;
  - System Security Authorization Agreement;
  - Standard Operating Procedures; and
  - Rules of Behavior.

- We tested procedures in place for screening and granting individuals access to DONBITS.

- We classified each control objective question as having "high," "medium," or "low" risk using the following definitions:

  - *High Risk* – Indicates we identified a significant control weakness – i.e., internal controls were missing or inadequate – that could potentially allow unauthorized access to, manipulation of, or destruction of electronic data within DONBITS;

  - *Medium Risk* – Denotes some internal controls existed; however, there is a residual risk of data being compromised and moderate concern still exists; and

  - *Low Risk* – Represents that effective internal controls were in place to protect data within DONBITS.

- We briefed our preliminary risk assessment results to DASN (IS&A), the system owner, on 18 December 2003 and made suggestions to mitigate the initial risks identified.

- We followed up with key DON personnel and support contractors and reviewed the corrective actions taken and adjusted our risk assessment accordingly.

We summarized the results from the risk ratings given to each question to rate each of the 17 specific control objectives or techniques and the following 3 major control areas:

- **Management Controls,** which focus on the management of the information technology security system and the management of risk for a system. They are techniques and concerns that are normally addressed by management.

- **Operational Controls,** which address security methods focusing on mechanisms primarily implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls.

- **Technical Controls,** which focus on security controls that the computer system executes. The controls can provide automated protection for unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data.

Exhibit C:

Pertinent Guidance

Office of Management and Budget Circular No. A-130[4] establishes policy for the management of Federal information resources**.** Appendix III of the circular, "Security of Federal Automated Information Resources," establishes a minimum set of controls to be included in Federal automated information security programs to provide adequate security. "Adequate security" means security commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information. These include assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls. The circular also states that the security plan shall be consistent with guidance issued by NIST.

DoD Instruction 5200.40[5] establishes a standard DoD-wide process, a set of activities, general tasks, and a management structure to certify and accredit information systems that will maintain the information assurance and security posture of the Defense Information Infrastructure. DITSCAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information.

NIST Special Publication 800-26 utilizes an extensive questionnaire containing specific control objectives and techniques against which an unclassified system can be tested and measured for each of the 3 major control areas covering 17 topics. The questionnaire can be used as a guide for thoroughly evaluating the security of an agency's system.

[4] OMB Circular No. A-130, Management of Federal Information Resources, dated 8 February 1996.

[5] DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process," dated 30 December 1997.

Exhibit D:

Acronym and Definition List

Term	Definition
BRAC	**Base Realignment and Closure**
CCB	**Configuration Control Board.** The purpose of the CCB is to control major issues such as schedule, function, and configuration of the system as a whole. CCB supports the project manager and is composed of technical and administrative representatives who recommend approval or disapproval of proposed engineering changes to the software's current approved configuration and its documentation.
DASN (IS&A)	**Deputy Assistant Secretary of the Navy for Infrastructure Strategy and Analysis**
DITSCAP	**DoD Information Technology Security Certification and Accreditation Process.** The standard DoD process for identifying information security requirements, providing security solutions, and managing information system security activities.
DoD	**Department of Defense**
DON	**Department of the Navy**
DONBITS	**Department of the Navy Base Realignment and Closure 2005 Information Transfer System**
Federal Information System Control Audit Manual	The document the Government Accountability Office auditors and agency inspector generals use when auditing an agency.
FTP	**File Transfer Protocol.** A service that supports file transfer between local and remote computers.
HQMC	**Headquarters, Marine Corps**
HTTP	**Hypertext Transfer Protocol**. A protocol used to request and transmit files, especially web pages and web page components, over the Internet or other computer networks.
HTTPS	**Hypertext Transfer Protocol Secure.** By convention, addresses that require an SSL connection start with "https:" instead of "http:".
IAT	**Infrastructure Analysis Team.** IAT supports DASN (IS&A) and controls the development of DONBITS and the associated documentation, and protects the integrity of the process by ensuring that all data, considerations, and evaluations are treated as sensitive and internal to the process.

Term	Definition
IATO	**Interim Approval To Operate.** Temporary approval granted by a designated approving authority for an information system to process information based on preliminary results of a security evaluation of the system.
IAVA	**Information Assurance Vulnerability Alerts.** Generated whenever a critical vulnerability exists that poses an immediate threat to DoD and where acknowledgement and corrective action compliance must be tracked. Not all identified vulnerabilities and threats will warrant an IAVA.
Intrusion Detection System	A software application that can be implemented on host operating systems or as network devices to monitor activity that is associated with intrusions or insider misuse, or both.
IP address	**Internet Protocol address.** An identifier for a computer or device on a network. Networks route messages based on the IP address of the destination.
ISA	**Interconnection Security Agreement.** An agreement established between the organizations that own and operate connected information technology systems to document the technical requirements of the interconnection. The ISA also supports an MOA between the organizations.
ISSM	**Information Systems Security Manager.** Oversees the implementation of, and compliance with, the standards, rules, and regulations specified in the organization’s security policy.
ISSO	**Information System Security Officer.** The person responsible to the designated approving authority for ensuring the security of an information technology system is approved, operated, and maintained throughout its life-cycle in accordance with the SSAA.
IT	**Information Technology**
MAC address	**Media Access Control address.** A hardware address that uniquely identifies each node of a network.
MCEN	**Marine Corps Enterprise Network.** A subset of the Defense Information Systems Network, it interconnects Marine Corps commands and activities. A complex system of network operating systems and application software allows commands and activities to exchange information over MCEN and obtain access to other computer networks such as the Internet.
MCNOSC	**Marine Corps Network Operations and Security Command.** DONBITS connectivity is supplied by MCNOSC. It controls all routers and firewalls providing connectivity to the servers.
MD5	**Message Digest 5.** A one-way hash function, meaning that a message is converted into a fixed string of digits, also called a message digest. With a one-way hash function, one can compare a calculated message digest against a decrypted message digest with a public key to verify that the message hasn’t been tampered with. This comparison is called a “hashcheck.”

Term	Definition
MOA	**Memorandum of Agreement.** A document established between two or more parties to define their respective responsibilities in accomplishing a particular goal or mission. In this advisory, an MOA defines the responsibilities of two or more organizations in establishing, operating, and securing a system interconnection.
NAVAUDSVC	**Naval Audit Service**
NIST	**National Institute of Standards and Technology**
NMCI	**Navy Marine Corps Intranet**
OSD	**Office of the Secretary of Defense**
SharePoint	Windows SharePoint Services is a collection of services for Microsoft Windows Server 2003 that can be used to create team-oriented Web sites to share information and foster collaboration with other users on documents. Windows SharePoint Services can also be used as a development platform for creating collaboration and information-sharing applications.
Software Configuration Management	The discipline of identifying the configuration of a product at discrete points in time to systematically control changes to this configuration and maintain the integrity and traceability of this configuration throughout the product life cycle.
SOP	**Standard Operating Procedures**
SSAA	**System Security Authorization Agreement.** A formal agreement among the designated approving authority, the certification authority, the information technology system user representative, and the program manager. It is used throughout the entire DITSCAP to guide actions, document decisions, specify information technology security requirements, document certification tailoring and level-of-effort, identify potential solutions, and maintain operational systems security.
SSL	**Secure Sockets Layer.** Based on public key cryptography, SSL is used to generate a cryptographic session that is private to a web server and a client browser.
SSP	**System Security Plan.** The objectives of the DONBITS SSP are to: provide an overview of the security requirements of the system, describe the controls in place or planned for meeting those requirements, and delineate the responsibilities of all individuals who have access to the system.
UDP	**User Datagram Protocol.** A connectionless protocol that runs on networks. UDP provides very few error recovery services, offering instead a direct way to send and receive datagrams over a network. It is used primarily for broadcasting messages over a network.
VLAN	**Virtual Local Area Network.** A network of computers that behave as if they are connected to the same wire, even though they may actually be physically located on different segments of a Local Area Network (LAN). VLANs are configured through software rather than hardware, which makes them extremely flexible.

Exhibit E:

Final Risk Assessment Summary of Control Objective Questions and Associated Risks

Department of the Navy (DON) Base Realignment and Closure (BRAC) 2005 Information Transfer System (DONBITS)

NAVAL AUDIT SERVICE
FINAL RISK ASSESSMENT SUMMARY
OF
CONTROL OBJECTIVE QUESTIONS
AND ASSOCIATED RISKS

16 September 2004

Prepared for:

Deputy Assistant Secretary of the Navy
for Infrastructure Strategy and Analysis

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
I. Management Controls (Control Areas 01 through 05)		Low	
01. Risk Management		Low	
1.1.1 – Is the current system configuration documented, including links to other systems?	The current system configuration is documented in the System Security Plan (SSP) section 4.2.3.4, the Memorandum of Agreement (MOA), the Interconnection Security Agreement (ISA), and the System Security Authorization Agreement (SSAA) section 3.	Low	The current system configuration documented.
1.1.4 – Have threat sources, both natural and manmade, been identified?	Threat sources, both natural and manmade, are documented in the SSAA section 2.2.	Low	Threat sources, both natural and manmade, were identified.
1.2.2 – Has a mission/business impact analysis been conducted?	The mission/business impact analysis is documented in the SSP section 3.5 and the SSAA sections 1.2.2 and 1.2.3.	Low	A mission/business impact analysis was conducted.
02. Review of Security Controls		Low	
2.2.1 – Is there an effective and timely process for reporting significant weakness and ensuring effective remedial action?	The process for reporting significant weaknesses and ensuring effective remedial action is documented in the SSP sections 4.2.1.2, 4.2.1.1.1, 4.2.2.2.1; SSP Appendix B, Section V, 1.g; SSAA section 2.1, 6.3; the MOA; and Security Standard Operating Procedure (SOP) sections 4.1.5, 4.3.7, 4.3.8, 4.3.25, 4.3.26, 4.4.9, 4.4.10.	Low	An effective and timely process is in place for reporting significant weakness and ensuring effective remedial action.
03. Life Cycle		Low	
3.1.1 – Is the sensitivity of the system determined?	The sensitivity of the system is documented in the SSP sections 3.2-3.3 and the SSAA section 1.2.3.	Low	The sensitivity of Department of the Navy (DON) Base Realignment and Closure (BRAC) Information Transfer System (DONBITS) was determined.
3.1.2 – Does the	The SSAA section 5.2	Low	While the SSAA only

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
business case document the resources required for adequately securing the system?	documents personnel, but not funding for security. According to the System Manager, $400,000 was initially budgeted for Fiscal Year 2004. No budget documents provided.		documents personnel for security and not funding, it is clear that DONBITS and BRAC are a priority and will be funded.
3.1.3 – Does the Investment Review Board ensure any investment request includes the security resources needed?	No budget documents provided. See 3.1.2	Low	While the SSAA only documents personnel for security and not funding, it is clear that DONBITS and BRAC are a priority and will be funded.
3.1.4 – Are authorizations for software modifications documented and maintained?	The software configuration management documents the change management process. The audit team was granted access to DONBITS Development Team website after a demonstration by the Information System Security Officer (ISSO).	Low	Authorizations for software modifications documented and maintained on-line.
3.1.5 – Does the budget request include the security resources required for the system?	No budget documents provided. See 3.1.2	Low	While the SSAA only documents personnel for security and not funding, it is clear that DONBITS and BRAC are a priority and will be funded.
3.1.6 – During the system design, are security requirements identified?	Security requirements were identified in the SSP section 4.2.	Low	Security requirements were identified while designing the system.
3.1.7 – Was an initial risk assessment performed to determine security requirements?	Security documents provided by the contractor included an initial risk assessment. Initial Risk Summary Status was presented to Deputy Assistant Secretary of the Navy for Infrastructure Strategy and Analysis by the audit team on 18 December 2003.	Low	An initial risk assessment was performed to determine security requirements.
3.1.8 – Is there a written agreement with program officials on the security controls employed and residual risk?	The Interim Approval to Operate (IATO) serves as a written agreement of approval of security controls and acceptance of residual risk.	Low	There is a written agreement with program officials on the security controls employed and residual risk.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
3.1.9 – Are security controls consistent with and an integral part of the Information Technology (IT) architecture of the agency?	Security controls are documented in the SSP section 4.2, the SSAA section 2.1, the MOA, and the ISA. Marine Corps network documentation was also provided.	Low	Security controls are consistent with and an integral part of the IT architecture.
3.1.10 – Are the appropriate security controls with associated evaluation and test procedures developed before the procurement action?	Tests are documented. Security controls are documented in the SSP section 4.2, the SSAA section 2.1, the MOA, and the ISA. Marine Corps network documentation was also provided.	Low	Appropriate security controls were evaluated and tested before implementation.
3.1.11 – Do the solicitation documents (e.g., Request for Proposals) include security requirements and evaluation/test procedures?	Not Applicable – No active solicitation. Contract N47408-03-F-5287 was issued 27 August 2003.	Low	Not Applicable – No active solicitation.
3.1.12 – Do the requirements in the solicitation documents permit updating security controls as new threats/vulnerabilities are identified and as new technologies are implemented?	Not Applicable – No active solicitation. Contract N47408-03-F-5287 was issued 27 August 2003. See 3.1.11.	Low	Not Applicable – No active solicitation.
3.2.1 – Are design reviews and system tests run prior to placing the system in production?	All proposed enhancements are reviewed in the weekly DONBITS Configuration Control Board (CCB) meetings, after Developer review. The CCB approves, disapproves or defers changes. IT Testers test each change based on the Test Scenarios created and the application documentation updated for the release. If the change has any existing issues, the IT Tester writes a Test Incident Report (TIR) describing the problem found. Samples of test documentation were	Low	Design reviews and system tests are run prior to implementation and placing the system into production.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	provided.		
3.2.2 – Are the test results documented?	Samples of test documentation were provided.	Low	Test results are documented.
3.2.3 – Is certification testing of security controls conducted and documented?	A copy of the results from a vulnerability test performed by the contractor was provided. Specifically, Microsoft Baseline Security Analyzer was run on the production server and all security checks passed. Microsoft Baseline Security Analyzer is a free, best practices vulnerability assessment tool for the Microsoft platform that helps with the assessment phase of an overall security management strategy.	Low	Certification testing of security controls was conducted and documented.
3.2.4 – If security controls were added since development, has the system documentation been modified to include them?	Documents were updated during our review and are current.	Low	The system documentation has been modified to include security controls that were added since development.
3.2.5 – If security controls were added since development, have the security controls been tested and the system recertified?	Samples of test documentation were provided.	Low	Tests of security controls are documented.
3.2.6 – Has the application undergone a technical evaluation to ensure that it meets applicable federal laws, regulations, policies, guidelines, and standards?	Naval Audit Service (NAVAUDSVC) risk assessment is based on applicable federal laws, regulations, policies, guidelines, and standards. The Base Line Security Requirements Questionnaire is part of the Initial Risk Assessment completed by a contractor. The questionnaire contained 142 questions, tied to the Federal Information System Control Audit Manual and National Institute of Standards and Technology (NIST) guidance,	Low	Risk assessment indicates that DONBITS meets applicable federal laws, regulations, policies, guidelines, and standards.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	with answers (either “yes,” “no,” or “partial.” All “no”s and “partial”s have comments as to why) and was a document on the collaboration website.		
3.2.7 – Does the system have written authorization to operate either on an interim basis with planned corrective action or full authorization?	DONBITS has written authorization to operate on an interim basis. The IATO was signed on 18 June 2004.	Low	DONBITS has written authorization to operate on an interim basis.
04. Authorize Processing (Certification & Accreditation)		Low	
4.1.4 – Has a contingency plan been developed and tested?	A contingency plan was developed and tested. The system manager provided signed documentation of successful tests.	Low	A contingency plan was developed and tested.
4.1.5 – Has a system security plan been developed, updated, and reviewed?	During our review, the SSP was developed, updated, and reviewed. The SSP is current.	Low	SSP has been developed, updated, and reviewed.
4.1.7 – Are the planned and in-place controls consistent with the identified risks and the system and data sensitivity?	Less stringent controls in place for staging environment due to lack of sensitive data (no BRAC questions/ answers). Security controls for the live system are documented in the SSP section 4.2, the SSAA section 2.1, the MOA, and the ISA. Marine Corps network documentation was also provided.	Low	Controls are consistent with the identified risks and the system and data sensitivity.
4.1.8 – Has management authorized interconnections to all systems (including systems owned and operated by another program, agency, organization or contractor)?	Interconnections to other systems are documented in the SSP section 4.2.3.4, the MOA, the ISA, and the SSAA section 3. See 1.1.1.	Low	Management has authorized interconnections to all systems.
4.2.1 – Has management initiated	The high priority of DONBITS and BRAC has ensured	Low	Management has initiated prompt action to correct

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
prompt action to correct deficiencies?	prompt attention to deficiencies.		deficiencies.
05. System Security Plan		Low	
5.1.1 – Is the system security plan approved by key affected parties and management?	The IATO is written approval of the SSP.	Low	Key affected parties and management approve the SSP.
II. Operational Controls (Control Areas 06 through 14)		Low	
06. Personnel Security		Low	
6.1.1 – Are all positions reviewed for sensitivity level?	According to SSP section 4.2.3.1.5, a secret clearance is required for personnel working on DONBITS. Also, documentation was provided listing individuals working on the system and their clearance level.	Low	Positions were reviewed for security level and determined to require a secret clearance.
6.1.2 – Are there documented job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties?	Different roles and responsibilities are outlined in the DONBITS Support SOP 12.	Low	Job descriptions that accurately reflect assigned duties and responsibilities and that segregate duties are documented.
6.1.3 – Are sensitive functions divided among different individuals?	According to SSP section 4.2.3.1.3, sensitive functions are divided between the Database Administrator, System Administrator, and ISSO.	Low	Sensitive functions are divided among different individuals.
6.1.4 – Are distinct systems support functions performed by different individuals?	Systems support functions are documented in the DONBITS Support SOP 12 and the SSP section 4.2.3.1.3.	Low	Different individuals perform distinct systems support functions.
6.1.5 – Are mechanisms in place for holding users responsible for their actions?	Mechanisms in place for holding users responsible for their actions are documented in the Rules of Behavior (Acknowledgement of User Responsibilities) and SSP sections 4.2.1.3 and 4.2.2.2.7. Further, audit logs	Low	Mechanisms were in place.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	and trails ensure accountability.		
6.1.6 – Are regularly scheduled vacations and periodic job/shift rotations required?	According to the system manager, the group is too small for rotations.	Low	While the staff is too small for rotations, separation of duties (6.1.2-6.1.4) mitigates the risk.
6.1.7 – Are hiring, transfer, and termination procedures established?	Hiring, transfer, and termination procedures are documented in SSP section 4.2.3.1.1 and the Security SOP 4 sections 4.3.19 and 4.4.3.3.	Low	Hiring, transfer, and termination procedures were established.
6.1.8 – Is there a process for requesting, establishing, issuing, and closing user accounts?	The process for requesting, establishing, issuing, and closing user accounts is documented in the SSP section 4.2.3.1.1, "Processing of DONBITS Applications" memorandum, and the DONBITS Support SOP 12.	Low	There is an effective process for requesting, establishing, issuing, and closing user accounts.
6.2.1 – Are individuals who are authorized to bypass significant technical and operational controls screened prior to access and periodically thereafter?	Screening policy is documented in the Security SOP 4 and the SSP section 4.2.3.1.5. A secret clearance is required for personnel working on DONBITS. Further, a spreadsheet was provided listing individuals working on the system and their clearance level.	Low	Individuals who are authorized to bypass significant technical and operational controls are required to have a secret clearance.
6.2.2 – Are confidentiality or security agreements required for employees assigned to work with sensitive information?	Users and developers sign non-disclosure agreements. A security agreement is also part of the user request form process.	Low	Users signed confidentiality and security agreements prior to working with sensitive information.
6.2.3 – When controls cannot adequately protect the information, are individuals screened prior to access?	Screening policy is documented in the Security SOP 4 and SSP section 4.2.3.1.5. A secret clearance is required for personnel working on DONBITS. Further, a spreadsheet was provided listing individuals working on the system and their clearance level.	Low	Individuals who are authorized to bypass significant technical and operational controls are required to have a secret clearance.
6.2.4 – Are there conditions for allowing	Users are not allowed system access prior to completion of	Low	Users are not allowed system access prior to

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
system access prior to completion of screening?	screening since the sensitivity of data and criticality of DONBITS demand high level of trust and security.		completion of screening.
07. Physical and Environmental Protection		Low	
7.1.1 – Is access to facilities controlled through the use of guards, identification badges, or entry devices such as key cards or biometrics?	Pentagon and National Capital Region badges are used for access to the computer room. The badges are not color coded for the three access levels (i.e., big room, main server room, and secure room). Visitors without clearances can be escorted. Secret clearances are required to enter unescorted. Pass codes can be required, but that feature is not currently used. The badge scanner logs the date and time a badge is swiped. A camera photographs the person scanning the badge.	Low	Access to facilities controlled through the use of identification badges with magnetic strips.
7.1.2 – Does management regularly review the list of persons with physical access to sensitive facilities?	The security office maintains a current list of persons with physical access to the computer room that is reviewed and signed by the Information Systems Security Manager (ISSM). The visitor log is manual rather than automated due to the signature requirement. Separate rosters are maintained for each room (main room, server room, and Top Secret switch room).	Low	Management regularly reviews the list of persons with physical access to sensitive facilities.
7.1.3 – Are deposits and withdrawals of tapes and other storage media from the library authorized and logged?	An electronic log is maintained to track tapes. A sample of this electronic log and an explanation of the process were received.	Low	Deposits and withdrawals of tapes from the library are authorized and logged.
7.1.4 – Are keys or other access devices needed to enter the computer room and tape/media library?	Tapes are kept in a locked fire resistant safe in a secure room within a controlled space.	Low	Keys and other access devices are needed to enter the computer room and tape/media library.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
7.1.5 – Are unused keys or other entry devices secured?	The primary tape custodian has a key to the fire resistant container used to store backups. The secondary tape custodian has the spare key.	Low	Unused keys are secured.
7.1.6 – Do emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter after fire drills, etc?	During an emergency, personnel can exit the computer room, but the doors lock behind them.	Low	Emergency exit and re-entry procedures ensure that only authorized personnel are allowed to re-enter the computer room.
7.1.7 – Are visitors to sensitive areas signed in and escorted?	There is a logbook in the big room for visitors to sign in. Visitors are required to sign in the logbook and to have an authorized escort while in the computer room.	Low	Visitors to sensitive areas are signed in and escorted.
7.1.8 – Are entry codes changed periodically?	Not Applicable	Low	Currently no entry codes are used. Swipe badge access is used instead.
7.1.9 – Are physical accesses monitored through audit trails and apparent security violations investigated and remedial action taken?	All badges are logged in with time/date stamp. If unauthorized use is caught on camera, the individual(s) will be reprimanded. The incident response process is documented in the Headquarters, U.S. Marine Corps (HQMC) Data Center SSAA section 4.3.11.	Low	Physical accesses are monitored through audit trails and apparent security violations are investigated and remedial action taken.
7.1.10 – Is suspicious access activity investigated and appropriate action taken?	System Security officer is notified of any system security vulnerabilities. The incident response process is documented in the HQMC Data Center SSAA section 4.3.11.	Low	Suspicious access activity is investigated and appropriate action taken.
7.1.11 – Are visitors, contractors and maintenance personnel authenticated through the use of preplanned appointments and identification checks?	Prior to visits to the HQMC Data Center, an appointment is required, "need to know" must be demonstrated, and approval of ISSM or the Security Officer must be obtained. Contractors must send their site visit request directly to the ISSM. Identification badges are	Low	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	checked prior to visitors signing in.		
7.1.12 – Are appropriate fire suppression and prevention devices installed and working?	Fire Marshall does checks for pressure, etc. In the case of fire, individual sprinklers go off rather than the entire system. A signed and dated copy of the Fire Alarm Submittal was received.	Low	Appropriate fire suppression and prevention devices are installed and working.
7.1.13 – Are fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, reviewed periodically?	The Fire Marshal's periodic checks include review for fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson. A signed and dated copy of Fire Alarm Submittal was received.	Low	Fire ignition sources, such as failures of electronic devices or wiring, improper storage materials, and the possibility of arson, are reviewed periodically.
7.1.14 – Are heating and air-conditioning systems regularly maintained?	Heating and air-conditioning systems are regularly maintained and checked every three months. Filters are changed and periodic maintenance is performed every six months. The audit team requested copy of the heating, ventilation, and air-conditioning (HVAC) certification and maintenance record from HQMC personnel.	Low	Heating and air-conditioning systems are regularly maintained, but the reviews should have been documented. As of the date of this report, we had not received the HVAC certification or maintenance record from HQMC personnel.
7.1.15 – Is there a redundant air-cooling system?	Two water-chilled air-conditioning units cool the big room in the HQMC Data Center. If the server room loses air-conditioning, the big room would automatically vent cold air into the server room.	Low	A redundant air-cooling system exists.
7.1.16 – Are electric power distribution, heating plants, water, sewage, and other utilities periodically reviewed for risk of failure?	Utilities fall under building maintenance. The audit team requested copy of the certification and maintenance record from HQMC personnel.	Low	Electric power distribution, heating plants, water, sewage, and other utilities are periodically reviewed for risk of failure and should have been documented. As of the date of this report, we had not received a certification or maintenance record from HQMC personnel.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
7.1.17 – Are building plumbing lines known and do not endanger system?	During renovation, personnel checked for water lines and none were found. In addition, the ceiling was sealed to prevent leaks.	Low	Building plumbing lines are known and do not endanger system.
7.1.18 – Has an uninterruptible power supply or backup generator been provided?	The system has an uninterruptible power supply that will last for one hour and a back-up generator. Both were utilized during Hurricane Isabel in September 2003 and the computer room remained operational.	Low	An uninterruptible power supply and backup generator are in place and operational.
7.1.19 – Have controls been implemented to mitigate other disasters, such as floods, earthquakes, etc.?	The network remained operational in September 2003 during Hurricane Isabel. The risk of other natural disasters, including flood and earthquake, is minimal.	Low	Controls have been implemented to mitigate disasters.
7.2.1 – Are computer monitors located to eliminate viewing by unauthorized persons?	Due to the angle of the monitors, an individual must be inside the computer room to view the computer monitors. Since only authorized persons are only allowed in the computer room, they are adequately protected.	Low	Computer monitors are located to eliminate viewing by unauthorized persons
7.2.2 – Is physical access to data transmission lines controlled?	Connections outside the room are fiber optic cable, which can't be tapped like copper wire. Sensitive data is encrypted. Areas with copper wire are locked. Ports (jacks) are disabled by HQMC Data Center and individuals must call to have them enabled.	Low	Physical access to data transmission lines is controlled.
7.3.1 – Are sensitive data files encrypted on all portable systems?	Not Applicable	Low	There are no laptops being used as a DONBITS server. No laptops or workstations can access the DONBITS Virtual Local Area Network (VLAN) directly.
7.3.2 – Are portable systems stored securely?	Not Applicable	Low	There are no laptops being used as a DONBITS server. No laptops or workstations can access the DONBITS

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
			VLAN directly.
08. Production, Input/Output Controls		Low	
8.1.1 – Is there a help desk or group that offers advice?	There is an Infrastructure Analysis Team (IAT) help desk for content questions and a DONBITS help desk for connectivity issues.	Low	There are two distinct help desks that offer advice.
8.2.1 – Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?	The processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information are documented in the on-line training, Rules of Behavior (Acknowledgement of User Responsibilities), and the Security SOP 4.	Med.	Processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information exist. However, the burden of responsibility is on the user to read, comprehend, and following the on-line training and Rules of Behavior.
8.2.2 – Are there processes for ensuring that only authorized users pick up, receive, or deliver input and output information and media?	According to the final “Data Transfer Process Improvement Paper” Secure Sockets Layer (SSL) over Hypertext Transfer Protocol Secure (HTTPS) is utilized to automate the transfer of data to OSD.	Low	SSL provides assurance that only authorized users receive, or deliver input and output information and media.
8.2.3 – Are audit trails used for receipt of sensitive inputs/outputs?	Print jobs are tracked. No other media exists since this is an automated system. Therefore, it is up to users to safeguard printouts.	Med.	Audit trails for receipt of sensitive inputs/outputs exist. However, the burden of responsibility is on the user to read, comprehend, and follow the on-line training and Rules of Behavior.
8.2.4 – Are controls in place for transporting or mailing media or printed output?	Print jobs are tracked. No other media exists since this is an automated system. Therefore, it is up to users to safeguard printouts. See 8.2.3.	Med.	Controls are in place for transporting or mailing media or printed output. However, the burden of responsibility is on the user to read, comprehend, and follow the on-line training and Rules of Behavior.
8.2.5 – Is there internal/external labeling [of media] for sensitivity?	According to the Security SOP 4 section 4.3.10, printouts are automatically labeled with the Deliberative Document statement.	Low	Media is labeled with the Deliberative Document statement.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
8.2.6 – Is there external labeling [of media] with special handling instructions?	According to Security SOP 4 section 4.3.10, printouts are automatically labeled with the Deliberative Document statement. See 8.2.5.	Low	Media is labeled with the Deliberative Document statement.
8.2.7 – Are audit trails kept for inventory management?	The inventory in Appendix C of the SSP includes serial numbers.	Low	Audit trails are kept for inventory management.
8.2.8 – Is media sanitized for reuse?	The process for sanitizing media for reuse is documented in “DONBITS Production System Sanitization and Disposition of Media” SOP.	Low	Media sanitization and disposition policy is documented.
8.2.9 – Is damaged media stored and /or destroyed?	The process for storing and destroying damaged media is documented in “DONBITS Production System Sanitization and Disposition of Media” SOP.	Low	Damaged media is stored and destroyed according to policy.
8.2.10 – Is hardcopy media shredded or destroyed when no longer needed?	A shredder is on-site for destruction of hardcopy media that is no longer needed.	Low	Hardcopy media is shredded when no longer needed.
09. Contingency Planning		Med.	
9.1.1 – Are critical data files and operations identified and the frequency of file backup documented?	The frequency of file backup for all files is documented in the Backup and Recovery SOP 1 section 4.3.1. According to policy, incremental/partial backups are done daily and full backups are performed weekly.	Low	The frequency of file backup for all critical data files and operations is documented.
9.1.2 – Are resources supporting critical operations identified?	The inventory in Appendix C of the SSP identifies resources supporting critical operations.	Low	Resources supporting critical operations have been identified.
9.1.3 – Have processing priorities been established and approved by management?	Not Applicable	Low	DONBITS uses stand-alone hardware so there is not an issue with the Marine Corps as to bandwidth. The Marine Corps does not maintain bandwidth or assign processing priorities for each application.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
9.2.1 – Is the [contingency] plan approved by key affected parties?	The IATO is written approval of the contingency plan.	Low	Key affected parties approve the contingency plan.
9.2.2 – Are responsibilities for recovery assigned?	A dedicated system administrator was assigned responsibility for recovery.	Low	Responsibilities for recovery have been assigned.
9.2.3 – Are there detailed instructions for restoring operations?	Detailed instructions for restoring operations are documented in both the Backup and Recovery SOP 1 and the Production System Software Restore SOP 2.	Low	Detailed instructions for restoring operations are documented.
9.2.4 – Is there an alternate processing site; if so, is there a contract or interagency agreement in place?	The alternate processing site is located within the contractor's facility in Fairfax, VA. Contract N47408-03-F-5287 was issued 27 August 2003.	Med.	The contractor site is not a hot mirror site and will instead rely on weekly backup tapes. Therefore, all data that was entered into the system after creation of the last successful backup tape may be lost. Full backups are rotated off-site weekly. One week's worth of data may equal hundreds of thousands of data elements.
9.2.5 – Is the location of stored backups identified?	According to the Backup and Recovery SOP 1 section 4.4.1.6, full backups are rotated off-site weekly and stored in a locked fire-resistant safe at the contractor's facility located in Fairfax, VA. The audit team verified the process during a site visit to the contractor's facility.	Low	The location of stored backups was identified. Backups are stored off-site in a locked fire-resistant container.
9.2.6 – Are backup files created on a prescribed basis and rotated off-site often enough to avoid disruption if current files are damaged?	Incremental/partial backups are done daily and full backups are performed weekly. See 9.1.1. Full backups are rotated off-site weekly. See 9.2.5. The contractor maintains an electronic log of backup files. The system administrator provided an example of the electronic log and explanation of the process.	Low	Backup files are created on a prescribed basis and rotated off-site weekly.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
9.2.7 – Is system and application documentation maintained at the off-site location?	System and application documentation are maintained at the off-site location.	Low	System and application documentation are maintained at the off-site location.
9.2.8 – Are all system defaults reset after being restored from a backup?	When DONBITS is restored from backup tape, Windows 2003 is formatted with the same file system as before the failure. SOP 2 also has explicit instructions for reconfiguration.	Low	System defaults are reset after being restored from a backup.
9.2.9 – Are the backup storage site and alternate site geographically removed from the primary site and physically protected?	The primary and alternate sites are 14 miles apart.	Med.	While the current situation is better than being located in the same building, this is not in line with best business practices (50-plus miles).
9.2.10 – Has the contingency plan been distributed to all appropriate personnel?	SOPs, including the Backup and Recovery SOP 1, are distributed to appropriate personnel.	Low	The contingency plan has been distributed to all appropriate personnel.
9.3.1 – Is an up-to-date copy of the plan stored securely off-site?	Current documentation is maintained off-site.	Low	An up-to-date copy of the plan is stored securely off-site.
9.3.2 – Are employees trained in their roles and responsibilities?	The dedicated system administrator was trained.	Low	The dedicated system administrator was trained.
9.3.3 – Is the plan periodically tested and readjusted as appropriate?	The contingency plan was developed and tested. The System Manager provided signed documentation of successful tests.	Low	The contingency plan is periodically tested and readjusted as appropriate.
10. Hardware and System Software Maintenance		Low	
10.1.1 – Are restrictions in place on who performs maintenance and repair activities?	There is an access control list for the computer room and server room. See 7.1.2.	Low	Restrictions are in place on personnel that perform maintenance and repair activities.
10.1.2 – Is access to all program libraries restricted and controlled?	Tapes are kept in a locked fire resistant safe in a secure room within a controlled space. Keys and other access devices are needed to enter the computer room and tape/media library.	Low	Access to all program libraries is restricted and controlled.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
10.1.3 – Are there on-site and off-site maintenance procedures (e.g., escort of maintenance personnel, sanitization of devices removed from the site)?	Visitors, contractors, and maintenance personnel are authenticated through the use of preplanned appointments and identification checks. See 7.1.11. The media sanitization process is documented in the "DONBITS Production System Sanitization and Disposition of Media" SOP. See 8.2.8 and 8.2.9.	Low	There are on-site and off-site maintenance procedures.
10.1.4 – Is the operating system configured to prevent circumvention of the security software and application controls?	Documentation of SharePoint configuration was received.	Low	The operating system was configured to prevent circumvention of the security software and application controls.
10.1.5 – Are up-to-date procedures in place for using and monitoring use of system utilities?	Only system administrators have access to the system, not developers. System administrators have completed the screening process prior to being given access to the system. See 6.2.3. However, as an inherent risk, system administrators, as part of their job, have 100 percent access to the system.	Med.	As an inherent risk, system administrators, as part of their job, have 100 percent access to the system.
10.2.1 – Is an impact analysis conducted to determine the effect of proposed changes on existing security controls, including the required training needed to implement the control?	The CCB examines all proposed enhancements to the project software and approves, disapproves, or defers changes. The DONBITS ISSO validates that adequate security settings are implemented for version and production upgrades.	Low	The impact of proposed changes is analyzed to determine the effect on existing security controls.
10.2.2 – Are system components tested, documented, and approved (operating system, utility, applications) prior to promotion to production?	All proposed enhancements are reviewed in the weekly DONBITS Configuration Control Board (CCB) meetings, after Developer review. The CCB approves, disapproves or defers changes. IT Testers test each change based on the Test Scenarios created	Low	System components are tested, documented, and approved prior to moving from the staging environment to production.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	and the application documentation updated for the release. If the change has any existing issues, the IT Tester writes a Test Incident Report (TIR) describing the problem found. Samples of test documentation were provided. See 3.2.1 and 3.2.2.		
10.2.3 – Are software change request forms used to document requests and related approvals?	Configuration management uses a Change Tracking System (DONBITS Incident Tracker) to record the progress of a change as it proceeds through the change cycle. Proposed changes are assigned a unique identifier and logged into the DONBITS Incident Tracker.	Low	Software change requests and related approvals are documented on-line.
10.2.4 – Are there detailed system specifications prepared and reviewed by management?	The system specifications are reviewed by the System Manager and covered in various documents; e.g., SSP, SSAA, MOA, and SOPs.	Low	Detailed system specifications are prepared and reviewed by management.
10.2.5 – Is the type of test data to be used specified; i.e., live or made up?	Test data is made up for off-site servers to avoid release of live answers/questions.	Low	Test data is made up for off-site servers to avoid release of live answers/questions.
10.2.6 – Are default settings of security features set to the most restrictive mode?	Default settings of security features were set to the most restrictive mode. Documentation of SharePoint configuration was received. See 10.1.4.	Low	Default settings of security features were set to the most restrictive mode.
10.2.7 – Are there software distribution implementation orders including effective date provided to all locations?	Not Applicable	Low	Activities access DONBITS via web rather than receiving software updates locally. Software is not distributed. Release notes for each release tells users what changes have been made.
10.2.8 – Is there version control?	Version control is documented in the Configuration Management Plan section 3.2.5.	Low	Version control is maintained.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
10.2.9 – Are programs labeled and inventoried?	Programs are not labeled. However, due to the system backup process, individual programs are not loaded during the recovery process. The current system backup process is faster than reloading and configuring programs individually.	Low	Individual programs are not needed for the recovery process.
10.2.10 – Are the distribution and implementation of new or revised software documented and reviewed?	Not Applicable	Low	There is no distribution of software to activities. Implementation involves moving software from the staging environment to the production environment. Release notes for each release tells users what changes have been made.
10.2.11 – Are emergency change procedures documented and approved by management, either prior to the change or after the fact?	Not Applicable	Low	Emergency changes are not authorized. All changes must go through CCB.
10.2.12 – Are contingency plans and other associated documentation updated to reflect system changes?	The contingency plan and related documents were being modified throughout our review, as needed, and currently reflect system changes.	Low	The contingency plan and related documents are updated and reflect system changes.
10.2.13 – Is the use of copyrighted software or shareware and personally owned software/equipment documented?	There is no personal software or shareware in the system. Copies of license procurement were provided for purchased software.	Low	Software purchase was documented.
10.3.1 – Are systems periodically reviewed to identify and, when possible, eliminate unnecessary services (e.g., FTP, Hypertext Transfer Protocol (HTTP), mainframe supervisor calls)?	The system is reviewed constantly and unnecessary services are removed. Documentation of vulnerability tests was provided.	Low	The system is reviewed constantly and unnecessary services are removed.
10.3.2 – Are systems periodically reviewed for known vulnerabilities	Microsoft security updates are done. The system is current on all patches. Tests	Low	The system is periodically reviewed for known vulnerabilities and software

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
and software patches promptly installed?	results were received. The system passed the test for known vulnerabilities and security patches/updates.		patches are promptly installed.
11. Data Integrity		Low	
11.1.1 – Are virus signature files routinely updated?	Norton Antivirus Corporate Edition updates virus signature files constantly. The server automatically distributes updates to clients.	Low	Virus signature files are routinely updated. Automatic distribution helps ensure file updates are performed.
11.1.2 – Are virus scans automatic?	According to Section 4.2.2.4.1 of the SSP, anti-virus software, Norton Corporate Edition, is provided by HQMC Data Center that automatically scans files and periodically scans the servers. Transactions will be scanned when processed through the system.	Low	Automatic virus scans help eliminate need for human intervention.
11.2.1 – Are reconciliation routines used by applications; i.e., checksums, hash totals, record counts?	The system uses Message Digest 5 (MD5) authentication, which is a form of a reconciliation routine. Reconciliation is inherent to SSL process.	Low	Reconciliation routines are used by applications.
11.2.2 – Is inappropriate or unusual activity reported, investigated, and appropriate actions taken?	The Marine Corps Network Operations and Security Command (MCNOSC) is responsible for providing intrusion detection and reporting incidents. The notification process documented in the MOA.	Low	Inappropriate or unusual activity is reported, investigated, and appropriate actions taken.
11.2.3 – Are procedures in place to determine compliance with password policies?	All users must sign Rules of Behavior (Acknowledgement of User Responsibilities). Online training emphasizes proper procedures. Users are forced by system to create unique passwords and change them every 90 days. See 15.1.6 and 15.1.7.	Low	Procedures are in place to determine compliance with password policies.
11.2.4 – Are integrity verification programs	There is not an automated software program in place to	Low	An automated software program would be one more

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
used by applications to look for evidence of data tampering, errors, and omissions?	look for evidence of data tampering, errors, and omissions. However, evidence would show up in logs. The contractor log review process was observed and sample logs were received. Contractor logs are reviewed regularly with an internally developed tool. Monitoring of network logs was turned over to the Navy Marine Corps Intranet (NMCI) in February 2004. Integrity verification programs are not run internally. Finally, the external portion of the network is handled by MCNOSC. The Marine Corps Enterprise Network (MCEN) specific documentation regarding logging and intrusion detection was provided.		layer to defense in depth but may be cost prohibitive. Instead logs are used to look for evidence of data tampering, errors, and omissions. The lack of internal review by NMCI is a concern. However, system logs are reviewed regularly with an internally developed tool and MCNOSC maintains strict vigilance against external threats to the network. This defense-in-depth mitigates the risk of data tampering.
11.2.5 – Are intrusion detection tools installed on the system?	MCNOSC uses Real Secure, a commercially available intrusion detection system. Specific documentation on intrusion detection was provided.	Low	Intrusion detection tools are installed on the network.
11.2.6 – Are the intrusion detection reports routinely reviewed and suspected incidents handled accordingly?	MCNOSC reviews intrusion detection reports routinely and takes action. Specific documentation on intrusion detection was provided.	Low	Intrusion detection reports are routinely reviewed and suspected incidents are handled accordingly.
11.2.7 – Is system performance monitoring used to analyze system performance logs in real-time to look for availability problems, including active attacks?	The system contractor looks at file size and transaction times directly off the system. The audit team observed the contractor log review process and sample contractor logs were received. Monitoring of network logs was turned over to NMCI in February 2004. Yet to have an internal problem. Most problems are external, such as when a Defense Information Systems Agency line went down. Either way, if the network	Low	Contractor logs are reviewed regularly with an internally developed tool. The lack of real-time internal review by NMCI is a concern. However, MCEN controls over the external network connection mitigate this risk greatly.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	were running slowly, NMCI would look into it. MCNOSC uses EMC Corporation software to monitor event logs. MCEN specific documentation was provided.		
11.2.8 – Is penetration testing performed on the system?	We received a copy of the results from a vulnerability test run on the production server by the contractor using Microsoft Baseline Security Analyzer. All security checks passed. See 3.2.3. A test was performed on the Marine Corps system last year using SecureScan NX tool, which is a commercial vulnerability assessment tool. Vulnerability Mitigation Declaration was provided. According to the results a small number of risks were identified and corrective action was taken.	Low	Penetration testing was performed on the entire system including the production server and network.
11.2.9 – Is message authentication used?	The system uses MD5 authentication, which is inherent to the SSL process.	Low	Message authentication is used as a part of SSL.
12. Documentation		Low	
12.1.1 – Is there vendor-supplied documentation of purchased software?	All vendor-supplied documentation of purchased software is on-line and available from any computer with Internet access.	Low	Vendor-supplied documentation of purchased software is available on-line.
12.1.2 – Is there vendor-supplied documentation of purchased hardware?	Vendor-supplied documentation came with the server boxes. However, it only covers general information like turning the power on.	Low	Vendor-supplied documentation came with purchased hardware.
12.1.3 – Is there application documentation for in-house applications?	Final documentation for the in-house application was received.	Low	Documentation for the in-house application exists.
12.1.4 – Are there network diagrams and documentation on setups of routers and switches?	The Marine Corps maintains network diagrams and documentation on setups of routers and switches. A sample was provided.	Low	Network diagrams and documentation on setups of routers and switches exist.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
12.1.5 – Are there software and hardware testing procedures and results?	Samples of test documentation were provided. See 3.2.1.	Low	Design reviews and system tests are run prior to implementation and placing the system into production.
12.1.6 – Are there standard operating procedures for all the topic areas covered in this document?	Controls discussed in the SSP and the SSAA are covered by various SOPs.	Low	Controls discussed in the SSP and the SSAA are covered by various SOPs.
12.1.7 – Are there user manuals?	User training manuals are posted on the DONBITS website.	Low	User manuals exist.
12.1.8 – Are there emergency procedures?	Emergency procedures are documented in both the Backup and Recovery SOP 1 and the Production System Software Restore SOP 2. The System Manager provided signed documentation of successful tests of these procedures.	Low	Emergency procedures are documented and tested.
12.1.9 – Are there backup procedures?	Backup procedures are documented in the Backup and Recovery SOP 1. The System Manager provided signed documentation of successful tests of these procedures.	Low	Backup procedures are documented and tested.
12.2.1 – Is there a system security plan?	An approved SSP exists. See 5.1.1.	Low	An SSP exists.
12.2.2 – Is there a contingency plan?	The contingency plan is documented in both the Backup and Recovery SOP 1 and the Production System Software Restore SOP 2. The System Manager provided signed documentation of successful tests of these procedures.	Low	The contingency plan is documented and tested.
12.2.3 – Are there written agreements regarding how data is shared between interconnected systems?	The final signed MOA with Marine Corps was received.	Low	There is a signed, written agreement regarding how data is shared between interconnected systems.
12.2.4 – Are there risk assessment reports?	A contractor and NAVAUDSVC performed initial risk assessments.	Low	Risk assessment reports were used to identify weaknesses and to establish

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	See 3.1.7 In addition, documentation was received of tests performed by the contractor and Marine Corps. See 11.2.8 Through these documents, risks were identified and controls were established accordingly.		controls.
12.2.5 – Are there certification and accreditation documents and a statement authorizing the system to process?	DONBITS has written authorization to operate on an interim basis. The IATO was based on the contents of all applicable certification and accreditation documents.	Low	Signed IATO is written authorization for the system to operate based on the contents of all applicable certification and accreditation documents.
13. Security Awareness, Training, and Education		Low	
13.1.1 – Have employees received a copy of the Rules of Behavior?	Rules of Behavior (Acknowledgement of User Responsibilities) are part of the DONBITS User Access Application and Non-Disclosure Agreement.	Low	Users receive a copy of the Rules of Behavior.
13.1.2 – Are employee training and professional development documented and monitored?	The ISSO received training and provided the respective Form 1556 and Certificate of Completion.	Low	Employee training and professional development are documented and monitored.
13.1.3 – Is there mandatory annual refresher training?	No mandatory annual refresher training is anticipated since the system life may be less than one year.	Low	No mandatory annual refresher training is anticipated since the system life may be less than one year.
13.1.4 – Are methods employed to make employees aware of security; i.e., posters, booklets?	Employees are made aware of security through internal IAT training.	Low	Employees are made aware of security through internal IAT training.
13.1.5 – Have employees received a copy of or have easy access to agency security procedures and policies?	Agency security procedures and policies are part of the Rules of Behavior (Acknowledgement of User Responsibilities) covered in the DONBITS User Access Application and Non-Disclosure Agreement. See 13.1.1.	Low	Users receive a copy of the agency security procedures and policies.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
14. Incident Response Capability		Low	
14.1.1 – Is a formal incident response capability available?	Formal incident response procedures are documented in the Security SOP 4 and the MOA. For DONBITS, the ISSO would call the Program/System Manager. The Program/System Manager would then call the Marine Corps representative. For the Marine Corps, the incident response process is documented in the HQMC Data Center SSAA section 4.3.11.	Low	Formal incident response capability is available.
14.1.2 – Is there a process for reporting incidents?	The process for reporting incidents is documented in the Security SOP 4 and the MOA. For DONBITS, the ISSO would call the Program/System Manager. The Program/System Manager would then call the Marine Corps representative. For the Marine Corps, the incident response process is documented in the HQMC Data Center SSAA section 4.3.11. See 14.1.1.	Low	The process for reporting incidents is documented.
14.1.3 – Are incidents monitored and tracked until resolved?	Incidents are monitored and tracked in the Software Incidence Response Log via the contractor established website. The ISSO reviews this log and attends weekly CCB meetings to discuss incidents and proposed resolution. A screenshot is included in the Security SOP 4 section 4.4.11.6.	Low	Procedures are documented to help ensure incidents are monitored and tracked properly until resolved.
14.1.4 – Are personnel trained to recognize and handle incidents?	Personnel know how to recognize and handle incidents through training and SOPs.	Low	Personnel are trained to recognize and handle incidents.
14.1.5 – Are alerts/advisories received and responded to?	Not Applicable	Low	As of our review, there were no Information Assurance Vulnerability Alerts (IAVAs) to date. The Marine Corps would contact the System

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
			Manager if an IAVA were received.
14.1.6 – Is there a process to modify incident handling procedures and control techniques after an incident occurs?	The ISSO would be involved in modifying incident handling procedures and control techniques after an incident occurs. Software changes would go through the CCB.	Low	The ISSO would be involved in modifying incident handling procedures and control techniques after an incident occurs. Software changes would go through the CCB.
14.2.1 – Is incident information and common vulnerabilities or threats shared with owners of interconnected systems?	Sharing of incident information and common vulnerabilities or threats is outlined in the Security SOP 4 and the MOA. For DONBITS, the ISSO would call the Program/System Manager. The Program/System Manager would then call the Marine Corps representative. For the Marine Corps, the incident response process is documented in the HQMC Data Center SSAA section 4.3.11.	Low	Incident information and common vulnerabilities or threats are shared with owners of interconnected systems.
III. Technical Controls (Control Areas 15 through 17)		Low	
15. Identification and Authentication		Low	
15.1.1 – Is a current list maintained and approved of authorized users and their access?	The ISSO approves and maintains a current list of authorized users and their access.	Low	A current list of authorized users and their access is maintained and approved by the ISSO.
15.1.3 – Are access scripts with embedded passwords prohibited?	“Remember my password” feature cannot be turned off. If it were turned off, passwords would be sent in clear text but SSL encrypted.	Med.	Access scripts with embedded passwords are not prohibited. However this is a trade-off. The ISSO must rely on self-initiated on-line training to prevent use of this feature. In addition, this feature will lock out accounts when password change is required. According to SSP Section 4.2.5.1.2.1, DONBITS requires passwords to be changed every 90 days. Due to other controls taken

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
			into account, this control is medium overall.
15.1.4 – Is emergency and temporary access authorized?	Emergency or temporary access is not authorized. There are no backdoors to the system. This helps prevent circumvention of controls in an emergency.	Low	Emergency or temporary access is not authorized.
15.1.5 – Are personnel files matched with user accounts to ensure that terminated or transferred individuals do not retain system access?	Personnel files are maintained by the field activities. Removal of users from the system is one of the Frequently Asked Questions answered in the on-line training. The process for closing user accounts is documented in SSP section 4.2.3.1.1 and new user request form process guidance. See 6.1.8.	Low	There is an effective process for closing user accounts.
15.1.6 – Are passwords changed at least every ninety days or earlier if needed?	According to SSP Section 4.2.5.1.2.1, passwords must be changed 90 days after initial login or last password reset. This process was verified through an audit team member's account following an email regarding password expiration.	Low	Passwords must be changed at least every 90 days.
15.1.7 – Are passwords unique and difficult to guess (e.g., do passwords require alpha numeric, upper/lower case, and special characters)?	Users are forced by system to create unique, difficult-to-guess passwords. Passwords require alpha numeric, upper/lower case, and special characters. This control mechanism was verified through an audit team member's account.	Low	Passwords require alpha numeric, upper/lower case, and special characters. This helps prevent successful "dictionary attacks."
15.1.9 – Are passwords not displayed when entered?	According to Security Sop 4 Section 4.2.2.3 and SSP Section 4.2.5.1.1, passwords are not displayed (masked) when entered. This control mechanism was verified through an audit team member's account.	Low	Passwords are not displayed when entered. This helps prevent successful "shoulder surfing."
15.1.10 – Are there procedures in place for handling lost and	There is a "forgot my password" link on the website in case a password is lost or	Low	Procedures are in place for handling lost and compromised passwords.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
compromised passwords?	compromised. Users enter their shared secret and receive an email with a link to change their password.		
15.1.11 – Are passwords distributed securely and users informed not to reveal their passwords to anyone (social engineering)?	When requesting an account, a shared secret is sent directly to the ISSO for screening. Users must know their shared secret during initial login. At that point, a new user is automatically forced to create a password. Passwords are transmitted via SSL. See 15.1.12 The on-line training and Rules of Behavior (Acknowledgment of User Responsibilities) cover password security. See 11.2.3	Low	Passwords and shared secrets are distributed securely and users are informed not to reveal their passwords to anyone.
15.1.12 – Are passwords transmitted and stored using secure protocols/algorithms?	Passwords are transmitted via SSL.	Low	Passwords are transmitted using secure protocols/algorithms.
15.1.13 – Are vendor-supplied passwords replaced immediately?	Any default vendor-supplied passwords were changed.	Low	Vendor-supplied passwords were replaced.
15.1.14 – Is there a limit to the number of invalid access attempts that may occur for a given user?	There is a limit of three invalid access attempts that may occur for a given user. In addition, there is a 30-minute delay for resetting a password after a user is locked out.	Low	There is a limit of three invalid access attempts that may occur for a given user. This helps prevent some forms of attacks involving repeatedly trying different passwords in an attempt to gain entry.
16. Logical Access Controls		Low	
16.1.1 – Can the security controls detect unauthorized access attempts?	Real Secure can detect unauthorized access attempts on the network. MCEN specific documentation on logging and intrusion detection was provided. Personnel also use audit logs to detect unauthorized access attempts. The contractor log review process was observed and sample contractor logs	Low	Contractor logs are reviewed regularly with an internally developed tool. The lack of real-time internal review by NMCI is a concern. However, MCEN controls over the external network connection mitigate this risk greatly.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	were received. Monitoring of network logs was turned over to NMCI in February 2004, but external pings and scans are still a MCNOSC issue. For internal traffic, NMCI doesn't track pings to individual machines but would be alerted if someone were pinging a router or switch.		
16.1.2 – Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion?	Only system administrators have access to the system, not developers. System administrators have completed the screening process prior to being given access to the system. See 6.2.3. However, as an inherent risk, system administrators, as part of their job, have 100 percent access to the system.	Med.	As an inherent risk, system administrators, as part of their job, have 100 percent access to the system.
16.1.3 – Is access to security software restricted to security administrators?	Access to security software is restricted to authorized personnel.	Low	Access to security software is restricted to authorized personnel.
16.1.8 – If encryption is used, are there procedures for key generation, distribution, storage, use, destruction, and archiving?	Not Applicable	Low	SSL encryption is used, therefore keys are not stored.
16.1.9 – Is access restricted to files at the logical view or field?	Rights and permissions restrict access to files at the logical view or field.	Low	Rights and permissions restrict access to files at the logical view or field.
16.1.10 – Is access monitored to identify apparent security violations and are such events investigated?	Audit logs are used to identify apparent security violations. The contractor log review process was observed and sample contractor logs were received. Monitoring of network logs was turned over to NMCI in February 2004. NMCI has no firm process for investigating security violations but does have the ability to search by Internet Protocol (IP) address and	Low	Contractor logs are reviewed regularly with an internally developed tool. Lack of a written process for NMCI is a concern. However, MCEN controls over the external network connection mitigate this risk greatly.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	Media Access Control (MAC) address during an investigation. MCEN specific documentation on logging and intrusion detection was provided.		
16.2.1 – Has communication software been implemented to restrict access through specific terminals?	Ports (jacks) are disabled by HQMC Data Center and individuals must call to have them enabled. See 7.2.2	Low	Communication software has been implemented to restrict access through specific terminals.
16.2.2 – Are insecure protocols (e.g., User Datagram Protocol, FTP) disabled?	The system is reviewed constantly and unnecessary services are removed. Documentation of vulnerability tests was provided. See 10.3.1.	Low	The system is reviewed constantly and unnecessary services are removed.
16.2.3 – Have all vendor-supplied default security parameters been reinitialized to more secure settings?	All vendor-supplied default security parameters have been reinitialized to more secure settings to the extent possible.	Low	All vendor-supplied default security parameters have been reinitialized to more secure settings to the extent possible.
16.2.4 – Are there controls that restrict remote access to the system?	Not Applicable	Low	There is no remote access to the system.
16.2.5 – Are network activity logs maintained and reviewed?	Network logs are maintained and reviewed. The contractor log review process was observed and sample contractor logs were received. Monitoring of network logs was turned over to NMCI in February 2004. NMCI has bandwidth tools to monitor internally. The tools generate reports if there is a problem. NMCI also has a server system log. For the first 6 weeks, logs have all details. Logs can go back for years, but with less detail. Some NMCI personnel review their logs daily. However, others indicated that they look at logs approximately 4 hours every 3 months and that no one is specifically designated/dedicated to	Low	Contractor logs are reviewed regularly with an internally developed tool. Lack of uniformity among NMCI reviews/reviewers and timeliness is a concern. However, MCEN controls over the external network connection mitigate this risk greatly.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	reviewing logs. MCEN specific documentation on logging was provided.		
16.2.6 – Does the network connection automatically disconnect at the end of a session?	The network connection automatically disconnects at the end of a session.	Low	The network connection automatically disconnects at the end of a session.
16.2.7 – Are trust relationships among hosts and external entities appropriately restricted?	Not Applicable	Low	There are no trust relationships except with users logging in.
16.2.8 – Is dial-in access monitored?	Not Applicable	Low	There is no dial-in access.
16.2.9 – Is access to telecommunications hardware or facilities restricted and monitored?	MCNOSC hubs and routers are in locked closets. The audit team tested telephone closets outside HQMC Data Center during a site visit.	Low	Access to telecommunications hardware and facilities is restricted and monitored.
16.2.10 – Are firewalls or secure gateways installed?	The MCEN firewall is installed per Marine Corps standard. Specific firewall documentation was provided.	Low	A firewall is installed.
16.2.11 – If firewalls are installed, do they comply with firewall policy and rules?	The MCEN firewall is installed per Marine Corps standard. Specific firewall documentation was provided.	Low	The MCEN firewall is installed per Marine Corps standard.
16.2.12 – Are guest and anonymous accounts authorized and monitored?	Not Applicable	Low	Guest and anonymous accounts are not authorized. According to SSP Section 4.2.5.1, the system does not allow any form of anonymous access and all users are required to have a User ID.
16.2.13 – Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished?	There is a Department of Defense warning banner within the "privacy and security notice" link located on the DONBITS home page that warns users they have accessed a U.S. Government system and can be punished. However, this is not a popup log-on banner that requires users to click on an acceptance button before	Med.	An approved standardized log-on banner is not automatically displayed on the first page of the system requiring unauthorized users to acknowledge that they have accessed a U.S. Government system and can be punished. Having a popup banner gives the System Owner certain legal rights against both

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	being presented with the DONBITS login screen as stated in the SSP section 4.2.5.2.1, the Marine Corps Base Order 5230.3, dated 20 January 2000, and All Marine message 167/97, dated 19 May 1997. In lieu of a popup banner, the System Owner is relying on other controls in place to mitigate unauthorized access, e.g., the screening and approval process for granting user access accounts (See 6.2.4), MCNOSC's firewall and intrusion detection tools (See 11.2.6 and 16.1.1), and NMCI's daily monitoring of the network logs and interfacing with the ISSM (See 17.1.1).		unauthorized individuals and users who signed the documents in Appendix B of the SSP. According to System Manager, a popup banner will not be implemented. The System Owner accepts this level of risk based on the other controls in place to mitigate unauthorized access into DONBITS.
16.2.14 – Are sensitive data transmissions encrypted?	Sensitive data transmissions are encrypted using SSL.	Low	Sensitive data transmissions are encrypted using SSL.
16.2.15 – Is access to tables defining network options, resources, and operator profiles restricted?	Access to tables defining network options, resources, and operator profiles is restricted to the system administrator.	Low	Access to tables defining network options, resources, and operator profiles is restricted to the system administrator.
16.3.1 – Is a privacy policy posted on the web site?	A privacy policy is posted on the DONBITS website. The text of this notice was reviewed by NAVAUDSVC prior to posting to ensure it followed the Department of Defense Web Administration of 7 Dec 1998, Part V, Paragraph 4.	Low	A privacy policy is posted on the DONBITS website in accordance with applicable criteria.
17. Audit Trails		Low	
17.1.1 – Does the audit trail provide a trace of user actions?	For DONBITS, the audit trail exists at the certification chain only. DONBITS is not tracking every single keystroke of every single user. For the network, monitoring of network logs was turned over to NMCI in February 2004. NMCI	Low	Audit trails provide a trace of user actions.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	system administrators check logs daily and can monitor log-ins, accesses, and virus activity. NMCI system administrators interface with the ISSM and can trace down to the user-level.		
17.1.2 – Can the audit trail support after-the-fact investigations of how, when, and why normal operations ceased?	DONBITS logs can tell who certified. However, DONBITS is not tracking every single keystroke of every single user. The contractor log review process was observed and sample contractor logs were received. Monitoring of network logs was turned over to NMCI in February 2004. NMCI logs can support after-the-fact investigations.	Low	The audit trail can support after-the-fact investigations of how, when, and why normal operations ceased.
17.1.3 – Is access to online audit logs strictly controlled?	Only the server administrator has access to MCNOSC logs. Even the security officer must request the file.	Low	Access to online audit logs is strictly controlled.
17.1.4 – Are offline storage of audit logs retained for a period of time, and if so, is access to audit logs strictly controlled?	DONBITS logs are maintained in backups. Monitoring of network logs was turned over to NMCI in February 2004. The NMCI log server is not backed up. However, it is Solaris/Unix based rather than Windows NT. According to NMCI, there have been no problems with this server over the past three years.	Low	Offline storage of DONBITS audit logs is part of system backup and is strictly controlled. Technically NMCI audit logs could be inadvertently erased preventing future review of controls and/or incidents. However, due to problems being rare (none in past three years), this is a low risk.
17.1.5 – Is there separation of duties between security personnel who administer the access control function and those who administer the audit trail?	Only the server administrator has access to MCNOSC logs. Even the security officer must request the file. See 17.1.3.	Low	There is separation of duties between security personnel who administer the access control function and those who administer the audit trail.
17.1.6 – Are audit trails reviewed frequently?	DONBITS logs are reviewed daily during certification process. The contractor log review process was observed and sample contractor logs were received. Monitoring of	Low	Contractor logs are reviewed regularly with an internally developed tool. Lack of uniformity among NMCI reviews/reviewers and timeliness is a concern.

Risk Control Area / Question	Response / Comments	Rating	Rating Explanation
	network logs was turned over to NMCI in February 2004. NMCI personnel review their logs daily. However, the HQMC Lead Engineer indicated that he looks at his logs approximately 4 hours every 3 months. MCEN specific documentation on logging was provided.		However, MCEN controls over the external network connection mitigate this risk greatly.
17.1.7 – Are automated tools used to review audit records in real time or near real time?	DONBITS logs are reviewed manually. The contractor log review process was observed and sample contractor logs were received. Monitoring of network logs was turned over to NMCI in February 2004. NMCI scans are not automated. Instead, the HQMC Lead Engineer performs manual scans that filter out resolved error messages and hone in on certain machines. A word document describing this procedure was received. MCEN specific documentation on logging was provided.	Low	Contractor logs are reviewed regularly with an internally developed tool. Automated tool for NMCI would facilitate the process, making more frequent reviews possible. However, MCEN controls over the external network connection mitigate this risk greatly.
17.1.8 – Is suspicious activity investigated and appropriate action taken?	The process for investigating and taking appropriate action against suspicious activity is documented in the Security SOP 4 and the MOA. For DONBITS, the ISSO would call the Program/System Manager. The Program/System Manager would then call the Marine Corps representative. The Marine Corps incident response process is documented in the HQMC Data Center SSAA section 4.3.11. See 14.1.1.	Low	Suspicious activity is investigated and appropriate action is taken.
17.1.9 – Is keystroke monitoring used? If so, are users notified?	Not Applicable	Low	Keystroke monitoring is not used.

Exhibit F:

Discussion of Control Objective Questions Rated Medium Risk

During our assessment we used the answers for selected, pertinent questions contained in the **National Institute of Standards and Technology** NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, Appendix A, System Questionnaire to rate the risks associated with the information technology security assurance for the Department of the Navy (DON) Base Realignment and Closure (BRAC) 2005 Information Transfer System (DONBITS), provide feedback to lower the risk, evaluate corrective actions taken by the Infrastructure Analysis Team (IAT) and the DONBITS contractor to reduce the risk and re-evaluate the level of risk.

The NIST System Questionnaire, as amended, consisted of 191 control objective questions covering 17 topics across the 3 major control areas. Each topic contained critical elements and supporting security control objectives and techniques (questions) about the system. (See Exhibit E for the complete list of questions, comments, risk ratings and rating explanations) At the end of our review, we rated 9 control objective questions as presenting a medium risk to DONBITS and the data it stores. However, it is important to consider the entire information assurance strategy and all applicable controls when determining the overall level of risk. In many instances secondary controls helped to mitigate the risk to the system overall. Therefore, the Management, Operational, and Technical control areas and 16 of the 17 topic areas are rated as having a low vulnerability to unauthorized access to, manipulation of or destruction of electronic data within DONBITS despite a limited number of control objective questions presenting a medium risk. The following is a summary of the 9 control objective questions rated as medium risk:

Production, Input/Output Controls Area

1. **Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?**

Processes and procedures are documented in the on-line training, the Rules of Behavior and the Security Standard Operating Procedure. However, the burden of responsibility is on the user to read, comprehend, and follow the on-line training and Rules of Behavior. Each user has accepted responsibility for safeguarding all inputs to and/or outputs from DONBITS by signing the documents in Appendix B of the SSP.

2. Are audit trails used for receipt of sensitive inputs/outputs?

Audit trails for receipt of sensitive inputs/outputs exist. However, each user has accepted responsibility for safeguarding all inputs to and/or outputs from DONBITS by signing the documents in Appendix B of the SSP.

3. Are controls in place for transporting or mailing media or printed output?

Controls are in place for transporting or mailing media or printed output. However, as stated in the online training and Rules of Behavior, it is up to users to safeguard printouts and any information gathered to support the certified responses.

Contingency Planning

4. Is there an alternate processing site; if so, is there a contract or interagency agreement in place?

5. Are the backup storage site and alternate site geographically removed from the primary site and physically protected?

The alternate processing site is not a “hot site,” i.e., a fully operational off-site data processing facility equipped with hardware and system software to be used in the event of a disaster. Therefore, all data that was entered into the system after the creation of the last successful weekly backup tape, which could potentially be hundreds of thousands of data elements, may be lost. Additionally, the alternate processing site is 14 miles from the primary site, contrary to the recommended 50 or more miles distance. Although not the best situation, we do not believe it is feasible at this time to create a “hot site” or to move the alternate processing site further away.

Hardware and System Software Maintenance Area

6. Are up-to-date procedures in place for using and monitoring use of system utilities?

Only system administrators have access to the system. As part of their job, system administrators have 100 percent access to the system, and for that reason there is an inherent risk. However, system administrators have completed the screening and approval process prior to being given access to the system. Further, system administrators had accepted responsibility for safeguarding all inputs to and/or outputs from DONBITS by signing the documents in Appendix B of the SSP.

Identification and Authentication Area

7. Are access scripts with embedded passwords prohibited?

The “Remember my password” feature cannot be turned off without sending passwords in clear text. Given the choice, the System Owner elected not to send passwords in clear text and included a section in the on-line training that prohibited the use of the “Remember my password” feature. While the burden of responsibility is on the user to read, comprehend, and follow the on-line training and Rules of Behavior, as an added control measure, this feature locks out users every 90 days when their password is required to be changed. However, if the feature is checked, the potential still exists for anyone using that computer to gain access into DONBITS after an authorized user logs in to the system. Although a concern, this is not a high risk to the system.

Logical Access Controls Area

8. Is an approved standardized log-on banner displayed on the system warning unauthorized users that they have accessed a U.S. Government system and can be punished?

When an individual logs into DONBITS an approved standardized log-on banner is not displayed. There is a Department of Defense warning banner within the “privacy and security” notice link located on the DONBITS home page that warns users that they have accessed a U.S. Government system and can be punished. However, there is not an automatic popup log-on banner that requires the user to click on an acceptance button before being presented with the DONBITS login screen as stated in the SSP and as required by Marine Corps guidance. Having a popup banner gives the system owner certain legal rights against both unauthorized individuals and users who signed the documents in Appendix B of the SSP. We determined that the System Owner, in lieu of implementing a popup banner, is relying on other controls in place to mitigate unauthorized access (e.g., the screening and approval process for granting user access accounts; the Marine Corps Network Operations and Security Command’s firewall and intrusion detection tools; and the Navy/Marine Corps Intranet’s daily monitoring of the network logs and interfacing with the Information System Security Manager). The DASN (IS&A) has acknowledged and accepted this level of risk based on the other controls in place to mitigate unauthorized access into DONBITS.

9. Is there access control software that prevents an individual from having all necessary authority or information access to allow fraudulent activity without collusion?

Only system administrators have access to the system. As part of their job, system administrators have 100 percent access to the system, and for that reason there is an inherent risk. However, system administrators have completed the screening and approval process prior to being given access to the system. Further, system administrators had accepted responsibility for safeguarding all inputs to and/or outputs from DONBITS by signing the documents in Appendix B of the SSP.