



DEPARTMENT OF THE NAVY  
UNITED STATES NAVY BAND  
617 WARRINGTON AVE., SE  
WASHINGTON NAVY YARD, DC 20374-5054

NAVBANDINST 5239.1D  
NB.ISO  
15 JUN 2010

NAVY BAND INSTRUCTION 5239.1D

From: Commanding Officer/Leader, United States Navy Band

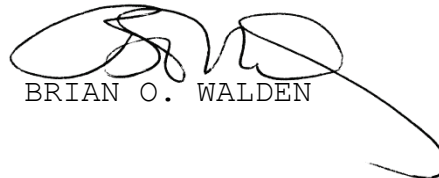
Subj: NAVY BAND COMMAND INFORMATION SYSTEMS SECURITY POLICY

Encl: (1) INFORMATION SYSTEMS SECURITY POLICY

1. Purpose. To promulgate Navy Band's Information Systems Security Policy.

2. Cancellation. NAVBANDINST 5239.1C.

3. Action. All supervisors using Navy Band Information Systems will ensure their personnel are informed of and adhere to enclosure (1).



BRIAN O. WALDEN

Distribution:  
Electronic, via intranet

INFORMATION ASSURANCE POLICY

for the

United States Navy Band

15 Jun 2010

## Table of Contents

<b>INTRODUCTION</b>	<b>5</b>
<b>1.1 PURPOSE</b>	<b>5</b>
<b>1.2 SCOPE</b>	<b>5</b>
<b>1.3 REFERENCES</b>	<b>5</b>
1.3.1 National-level policies, guidelines, and regulations	5
1.3.2 Service Specific policies, guidelines, and regulations	7
1.3.3 Other references	3
<b>1.4 ORGANIZATION</b>	<b>3</b>
<b>BACKGROUND</b>	<b>4</b>
<b>2.1 SYSTEM OVERVIEW</b>	<b>4</b>
<b>2.2 BRIEF CONCEPT OF OPERATIONS</b>	<b>4</b>
2.2.1 General Security Concerns	4
2.2.2 Use of Navy Band Information Systems	4
2.2.3 Personal Software	5
2.2.4 Copyright	5
2.2.5 End User Responsibilities	5
<b>2.3 THREAT ENVIRONMENT</b>	<b>6</b>
<b>2.4 UMBRELLA GUIDANCE</b>	<b>6</b>
<b>INFORMATION ASSURANCE OBJECTIVES</b>	<b>7</b>
<b>3.1 Information Assurance Properties</b>	<b>7</b>
3.1.1 Confidentiality	7
3.1.2 Integrity	7
3.1.3 Availability	7
<b>3.2 Specific Information Assurance Objectives</b>	<b>7</b>
3.2.1 Communications Security Objectives	8
3.2.2 Computer Security Objectives	8
3.2.2.1 Access Control	8
3.2.2.2 Object Reuse	9
3.2.2.3 Labels	9
3.2.2.4 Mandatory Access Control	9
3.2.2.5 Identification and Authentication	9
3.2.2.6 Security Audit	9
3.2.2.7 Architecture Assurance	10
3.2.2.8 Integrity Assurance	10
3.2.2.9 Testing Assurance	10

3.2.2.10	Documentation .....	10
3.2.2.11	Functional Integrity Protection .....	11
3.2.2.12	Data Integrity Protection .....	11
3.2.3	Personnel Security Objectives .....	11
3.2.4	Physical Security Objectives .....	11
3.2.5	Procedural Security Objectives .....	11
3.2.6	Security Education, Training, and Awareness Objectives .....	13
3.2.7	Operational Site Objectives .....	13
3.2.7.1	Accreditation .....	13
3.2.7.2	Management .....	14
3.2.7.3	DAA Role .....	14
3.2.7.4	IAM Role .....	15
3.2.7.5	Mode of Operation .....	16
<b>RATIONALE FOR SELECTED OBJECTIVES .....</b>		<b>17</b>
<b>4.1 INTRODUCTION .....</b>		<b>17</b>
<b>4.2 RATIONALE FOR SPECIFIC INFORMATION ASSURANCE OBJECTIVES .....</b>		<b>17</b>
4.2.1	Communications Security Objectives Rationale ...	17
4.2.2	Computer Security Objectives Rationale .....	17
4.2.2.1	Access Control Objectives Rationale .....	18
4.2.2.2	Object Reuse Objectives Rationale .....	18
4.2.2.3	Labels Objectives Rationale .....	18
4.2.2.4	Mandatory Access Control Objectives Rationale	18
4.2.2.5	Identification and Authentication Objectives Rationale .....	18
4.2.2.6	Security Audit Objectives Rationale .....	18
4.2.2.7	Architecture Assurance Objectives Rationale ..	18
4.2.2.8	Integrity Assurance Objectives Rationale .....	18
4.2.2.9	Testing Assurance Objectives Rationale .....	19
4.2.2.10	Specification and Verification Assurance Objectives Rationale .....	19
4.2.2.11	Documentation Objectives Rationale .....	19
4.2.2.12	Functional Integrity Protection Objectives Rationale .....	19
4.2.2.13	Data Integrity Protection Objectives Rationale .....	19
4.2.3	Personnel Security Objectives Rationale .....	19
4.2.4	Physical Security Objectives Rationale .....	19
4.2.5	Procedural Security Objectives Rationale .....	19
4.2.6	Security Education, Training, and Awareness Objectives Rationale .....	360
4.2.7	Operational Site Objectives Rationale .....	360
4.2.7.1	Accreditation Objectives Rationale .....	360
4.2.7.2	Management Objectives Rationale .....	360

4.2.7.3	DAA Role Objectives Rationale .....	360
4.2.7.4	IAM Role Objectives Rationale .....	20
4.2.7.5	Security Mode of Operation Objectives Rationale .....	20

## **SECTION 1**

### **INTRODUCTION**

#### **1.1 PURPOSE**

This document specifies the Information Assurance Policy (IAP) objectives for the Navy Band. The purpose of this IAP is to establish the set of laws, rules, and practices that control how information and resources must be protected with regard to confidentiality, integrity, and availability. In this way, this document defines mission security needs the Navy Band must address by either technical or non-technical objectives.

This document establishes command Information Assurance (IA) objectives derived from higher-level directives and instructions (e.g., Department of Defense, Department of the Navy, or civil agency), and the command's operational concept and threat assessment. The IAP represents an essential step in the Certification and Accreditation (C&A) of Navy Band owned systems. The IAP is developed without concern for the internal system architecture, system design, and system implementation details. These objectives are intended as the primary drivers for defining the IA requirements of the information system's architecture.

Each service or agency intending to implement an information system is required to develop a specific IAP which addresses their governing higher level information assurance instructions, concept of operations, and threat.

#### **1.2 SCOPE**

The IAP defined in this document applies to all Navy Band Information Systems. The Information Assurance objectives defined by this IAP specify the security necessary to protect the information and resources of the Navy Band.

#### **1.3 REFERENCES**

The references identified in the following subsections provided guidance and/or information that were considered during the development of this IAP.

##### **1.3.1 National-level policies, guidelines, and regulations**

- a. 10 U.S.C. Section 2224, Defense Information Assurance Program.  
<http://cio-nii.defense.gov/pocketref/output-9-0.html>
- b. 40 U.S.C. Section 5002 et. seq., The Information Technology Reform Act of 1996, "Clinger/Cohen Act,"  
3 January 1996.  
[http://www.cio.gov/Documents/it\\_management\\_reform\\_act\\_Feb\\_1996.html](http://www.cio.gov/Documents/it_management_reform_act_Feb_1996.html)
- c. CSC-STD-003-85, Computer Security Requirements --  
Guidance for Applying the Department of Defense Trusted  
Computer Security Evaluation Criteria in Specific  
Environments, 25 June 1985.  
<http://www.fas.org/irp/nsa/rainbow/std003.htm>
- d. DoD Instruction 5200.01, DoD Information Security  
Program and Protection of Sensitive Compartmented  
Information., 9 October 2008.  
<http://www.dtic.mil/whs/directives/corres/pdf/520001p.pdf>
- e. DoD 5200.1-R, DOD Information Security Program, 14  
January 1997.  
<http://www.dtic.mil/whs/directives/corres/pdf/520001r.pdf>
- f. DoD 5200.2-R, DoD Personnel Security Program (USDP),  
23 February 1996.  
<http://www.dtic.mil/whs/directives/corres/pdf/520002r.pdf>
- g. DoD Directive C-5200.5, Communications Security (COMSEC)  
(U), 21 April 1990.
- h. DoD Directive 8000.01, Management of the Department of  
Defense Information Enterprise, 10 February 2009.  
<http://www.dtic.mil/whs/directives/corres/pdf/800001p.pdf>
- j. DoD Directive 8100.02, Use of Commercial Wireless  
Devices, Services and Technologies in the Department of  
Defense (DoD) Global Information Grid (GIG), 23 April  
2007.  
<http://www.dtic.mil/whs/directives/corres/pdf/810002p.pdf>
- k. DoD Directive 8190.3, Smart Card Technology, 21 November  
2003.  
<http://www.dtic.mil/whs/directives/corres/pdf/819003p.pdf>

- l. DoD Directive 8500.01E, Information Assurance (IA), 23 April 2007.  
<http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf>
- m. DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003.  
<http://www.dtic.mil/whs/directives/corres/pdf/850002p.pdf>
- n. DoD Instruction 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling, 1 April 2004.  
<http://www.dtic.mil/whs/directives/corres/pdf/852002p.pdf>
- o. DoD Directive 8570.1, Information Assurance Workforce Improvement Program, 20 April 2010.  
<http://www.dtic.mil/whs/directives/corres/pdf/857001m.pdf>
- p. Executive Order 13292, Further Amendment to Executive Order 12958, as Amended, Classified National Security Information, 25 March 2003.  
<http://www.fas.org/sgp/bush/eoamend.html>
- q. Federal Information Security Management Act of 2002, Title III of E-Government Act of 2002 (PL 107-347), 7 January 2003.  
<http://csrc.nist.gov/drivers/documents/HR2458-final.pdf>
- r. National Security Directive (NSD)-42, National Policy for the Security of National Security Telecommunications and Information Systems, 5 July 1990.  
<http://www.fas.org/irp/offdocs/nsd/nsd42.pdf>
- t. National Security Telecommunications and Information Systems Security Instruction (NSTISSI) No. 4009, National Information Systems Security (INFOSEC) Glossary, September 2000.. <http://security.isu.edu/pdf/4009.pdf>
- u. National Security Telecommunications and Information Systems Security Directive (NSTISSD) 4002, Classification Guide for COMSEC Information, 5 June 1986.

### **1.3.2 Service Specific policies, guidelines, and regulations**

- a. OPNAVINST 5239.1C, Navy Information Assurance (IA) Program, 20 August 2008.  
<http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05->

200%20Management%20Program%20and%20Techniques%20Services/5239.1C.pdf

- b. SECNAVINST 5239.3B, Department of the Navy Information Assurance Policy, 17 June 2009.  
<http://doni.daps.dla.mil/Directives/05000%20General%20Management%20Security%20and%20Safety%20Services/05-200%20Management%20Program%20and%20Techniques%20Services/5239.3B.pdf>
- c. SECNAVINST M-5239.1, Department of the Navy Information Assurance Program, Information Assurance Manual, November 2005.  
<http://doni.daps.dla.mil/SECNAV%20Manuals1/5239.1.pdf>
- d. NAVSO Publication series 5239 addressing various elements of the Navy INFOSEC program.  
[http://www.fas.org/irp/doddir/navy/5239\\_xx.htm](http://www.fas.org/irp/doddir/navy/5239_xx.htm)
- e. Platform IT Guidance. 26 April 2010.  
[https://www.portal.navy.mil/netwarcom/NEWS/cio1/CIO1%20Documents/Documents%20under%20review/Review%20Completed/DON%20CIO%20-%20Platform%20IT%20\(PIT\)/DRAFT\\_Platform\\_IT\\_Guidance\\_v1\\_07\\_20081208.doc](https://www.portal.navy.mil/netwarcom/NEWS/cio1/CIO1%20Documents/Documents%20under%20review/Review%20Completed/DON%20CIO%20-%20Platform%20IT%20(PIT)/DRAFT_Platform_IT_Guidance_v1_07_20081208.doc)
- f. DON CIO Memo 02-10. Information Assurance Policy Update for Platform Information Technology. 26 April 2010.  
<http://www.doncio.navy.mil/PolicyView.aspx?ID=873>
- g. Platform Information Technology Definitions for the Department of the Navy. 27 November 2007.  
[http://www.doncio.navy.mil/uploads/Enclosure1\\_PlatformITDefinitionsforDON\[2\].pdf](http://www.doncio.navy.mil/uploads/Enclosure1_PlatformITDefinitionsforDON[2].pdf)
- h. Navy Platform Information Technology Checklist. 9 February 2009.  
<http://www.doncio.navy.mil/contentview.aspx?id=877>

### **1.3.3 Other references**

- a. CNSS Instruction 4009, National Information Assurance (IA) Glossary, 26 April 2010.  
[http://www.cnss.gov/Assets/pdf/cnssi\\_4009.pdf](http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf)

- b. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, <http://www.whitehouse.gov/omb/circulars/a130/a130trans4.html>

#### **1.4 ORGANIZATION**

The IAP for the Navy Band is organized as follows:

- a. Section 1 provides an introduction to the structure and content of this document.
- b. Section 2 provides background information necessary to understand and interpret the security guidance provided in the remainder of the document.
- c. Section 3 defines the high-level security goals and specific objectives that are applicable to the Navy Band.
- d. Section 4 provides the rationale for including the IA objective through a traceability table to the higher level directive, instruction, Concept of Operations, and/or threat assessment.

## SECTION 2

### BACKGROUND

#### 2.1 SYSTEM OVERVIEW

Navy Band does not administer a local area network (LAN) and maintains no connections to the Internet. These services are provided by the Navy and Marine Corps Intranet (NMCI), and network security is managed by the NMCI contractor. The Navy Band public web site is hosted on a shared server at the Defense Information Systems Agency (DISA) in Mechanicsburg, Pennsylvania through an annual contract for hosting and support services. The remaining Navy Band Information Systems can be divided by system function into six groupings:

**Archive workstation** - This is a MacIntosh workstation that has specialized software and hardware required for high quality digital archiving of Navy Band historical materials. This is a dedicated stand-alone machine that has no network or Internet connectivity.

**Arranger's workstations** - Considered "musical instruments", two of these systems are installed at the homes of Navy Band arranging staff and one is installed in the music library. These are stand-alone systems dedicated to music arranging. They have no other function and have no network or Internet connectivity.

**AV Department Sound Board Controllers** - These consist of one laptop computer and one tablet computer for each of the five performing units. The sole purpose of these systems is to evaluate and configure sound output settings for live performances. The laptop is connected via cable to the sound board, and the tablet communicates wirelessly with the laptop, enabling sound engineers to sample sound levels in different locations in the concert venue. These machines are dedicated to this function and do not connect to the network or Internet.

**Cruisers ensemble receptor controller** - This is a laptop that controls a receptor producing high fidelity synthesized musical instrument sounds that are used by a keyboardist in musical performances. The laptop also runs Logic Studio, which can produce additional sounds and a click-track. The

laptop is a dedicated system that has no other purpose and has no network or Internet connectivity.

**Recordings archive workstation** - This machine is dedicated to the digital archiving of sound recordings from Navy Band performances. It has specialized software and hardware for this purpose, and has no network or Internet connectivity.

**Recording Studio** - This system is used exclusively to process recorded music and is a completely dedicated component of the sound editing system. . It has no network or Internet connectivity.

All of the above systems process non-sensitive unclassified data only and pose no risk to government networks due to their dedicated mode of operation and lack of connectivity. The Archive workstation is the only system that processes non-musical data, and is therefore the only system that may meet the traditional definition of an automated information system (AIS). Any information that this system processes is carefully reviewed and approved by the Navy Band Public Affairs Office before it is made available to the public.

## **2.2 BRIEF CONCEPT OF OPERATIONS**

### **2.2.1 General Security Concerns**

Navy Band's stand-alone systems require Controlled Access Protection, User Identification and Authentication, and Discretionary Access Control, since unauthorized use could negatively impact mission accomplishment. The Archive workstation is located in a locked space, and is accessed only by authorized personnel with assigned accounts and passwords. The Arrangers workstations also require a user name and password for logon, with the Admin account controlled by ISO. The AV Department Sound Board Controller laptops are used exclusively by the Sound Engineers. Access is limited to those with authorized accounts and password logon is required. These laptops are stored in a locked office when not in use. The Cruisers receptor controller is used exclusively by the ensemble keyboardist and is also secured when not in use. The Recordings Archive machine is secured in a locked office, and used solely by the Tape Librarian. The Recording Studio workstation is located in a limited access area. These systems are unique in their function and require special

consideration, particularly with respect to contingency planning.

### **2.2.2 Use of Navy Band Information Systems**

All Navy Band Information Systems are for official use only. Use of government-owned equipment or software for unofficial or private business purposes is not authorized. Government software may be installed on personally owned computer equipment only if approved by the Information Assurance Manager (IAM) and the Information Systems Primary Responsible Officer (PRO) and a Government Software Usage Agreement is signed by the user.

### **2.2.3 Personal Software**

No software or utility of any kind may be installed on a Navy Band information system without the consent of the IAM and the Information Systems PRO. Downloading public domain/shareware software and software from unofficial sources onto government computers is prohibited. Installation of privately owned software or hardware on government equipment must be approved by the IAM, and a contractual agreement must be signed by the owner and the IAM. Open Source software may only be installed on a government system if it is Navy approved and authorized by the command IAM.

### **2.2.4 Copyright**

Navy Band Information Systems contain licensed software. Copying of licensed software for personal use is a violation of federal copyright law and is strictly forbidden. Similarly, the installation of a single software license on multiple systems unless authorized by the manufacturer is also a violation of federal law and is strictly forbidden.

### **2.2.5 End User Responsibilities**

Responsibility for the security of computer systems rests with each individual end user. Users must avoid fraud, waste, and abuse of information system resources and adhere to the following guidance:

- ✓ Support and promote good security practices
- ✓ Follow the established procedures of Navy Band's Information Assurance Program.

- ✓ Comply with all software copyright policies and never use unapproved software.
- ✓ Log off when leaving a computer workstation.
- ✓ Scan all portable media prior to using them on any Navy Band system.
- ✓ Avoid leaving sensitive data in any unrestricted area.
- ✓ Never process Classified or extremely sensitive data on any Navy Band computer system..
- ✓ Make backup copies of all critical data files and applications.
- ✓ Report all security incidents and violations to the IAM.

### **2.3 THREAT ENVIRONMENT**

Threat consists of defining the assets (i.e., information and resources), agents (i.e., Threat Agents), their activities (i.e., Threat Activity), their intent (i.e., disclosure, modification, denial of service), their capability (i.e., knowledge and technology), and their motivation (i.e., likelihood of success without consequences). Threat Agents can be categorized as Authorized Users, Unauthorized Users, or Manmade Events. Threat Activity is a Threat Agent's attempt to use a vulnerability of an information system to disclose, modify, or deny the access to or use of information and resources. Threat activities are many. Some of these activities include: Corruption, Exposure, Falsification, Incapacitation, Inference, Interception, Intrusion, Masquerade, Misappropriation, Misuse, Obstructions, and Repudiation. The Threat Assessment considers the capability and motivation of the Threat Agent in determining the required information assurance objectives to protect the assets.

### **2.4 UMBRELLA GUIDANCE**

Direction for information assurance is provided by the Department of Defense in DoDD 8500.1, Information Assurance. This directive establishes policy and describes the requirements for securing an information system. The Navy Band IAP identifies the IA objectives drawn from the higher-level umbrella guidance. These objectives shall be used to drive the development of IA requirements for application to Navy Band Information Systems and their environment.

## **SECTION 3**

### **INFORMATION ASSURANCE OBJECTIVES**

#### **3.1 INFORMATION ASSURANCE Properties**

The IA objectives for the Navy Band are established to achieve the three IA goals for information systems. These IA properties are confidentiality, integrity, and availability. Technical (i.e., Communications Security (COMSEC), Computer Security (COMPUSEC), and Compromising Emanations (TEMPEST)), and non-technical (i.e., Personnel Security (PERSEC), Physical Security (PHYSEC), Procedural Security (PROSEC), and Security Education, Training, Awareness, and Professionalization (SETAP)) IA disciplines provide the measures necessary for achieving the IA goals. None of these disciplines have precedence over any other; they must be understood together before any assessment of information protection can be achieved. Additionally, the categorization is not meant to imply an architecture but to draw from the discipline's objectives the capability for providing countermeasures to prevent the violation of an IA requirement.

DODI 8500.2 para. E4.1.1 defines Mission Assurance Categories and Confidentiality Levels and their corresponding information assurance controls. All Navy Band information systems are MAC III/Sensitive.

##### **3.1.1 Confidentiality**

Confidentiality refers to the concept of holding sensitive data in confidence, limited to an appropriate set of individuals or organizations.

The following goal defines the general need for confidentiality protection for the Navy Band:

The highest level of information handled by Navy Band systems is Privacy Data categorized under the Department of Defense (DOD) sensitivity marking system as Sensitive. Under DOD regulations, this information must be protected and only disclosed to individuals and entities who have an established need-to-know.

### **3.1.2 Integrity**

Integrity refers to the concept of keeping information and resources in a state of sound, unimpaired, or perfect condition, and preventing unauthorized alteration. One of the primary integrity functions of the Navy Band is to ensure the correct operation of the hardware and software.

### **3.1.3 Availability**

Availability refers to the state of ensuring that information and resources are in place and ready for use when needed to perform the mission and provided in time to be used to perform that mission. Protection must be provided to ensure all Navy Band Information Systems remain available and capable of satisfying Navy Band mission requirements.

## **3.2 Specific Information Assurance Objectives**

The specific IA objectives specified in this section interpret the IA properties of confidentiality, integrity, and availability required for the protection of Navy Band Information Systems.

### **3.2.1 Communications Security Objectives**

According to DODI 8500.2, para. E4.A5, DCSR-2, controls must be in place to protect sensitive information "when the information transits public networks or the system handling the information is accessible by individuals who are not authorized to access the information on the system." Sensitive information transmitted via email must be encrypted.

### **3.2.2 Computer Security Objectives**

#### **3.2.2.1 Access Control**

- a. Access control mechanisms shall be used to restrict the access of users, processes, and other external entities (including non-information system users) to sensitive information, functions, and services.
- b. Access control shall, either by explicit user action or by default, provide that objects are protected from unauthorized access.

- c. Access control shall be capable of including or excluding access to the granularity of a single user.
- d. Access control between identified and authenticated users and named objects shall be defined and implemented.
- e. An owner will be identified for each file or data collection throughout the information systems life cycle. Should the object owner's access to the system be terminated, then ownership will default to the system administrator.
- f. The file or data collection accessibility, maintenance, movement, and disposition shall be governed by security clearance, formal access approval, and need-to-know. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals, or defined groups of individuals, or by both.
- g. Only the command IAM shall assign access permission to an object by users not already possessing access permission.
- h. Controls shall be provided that limit the propagation of access rights.
- i. The principle of least privilege shall be used to limit the access of the users to system functions and services. Users shall only be granted access to the functions and services that they need to perform their assigned functions.
- j. The need-to-know principle shall be used to limit the access of users to information stored and processed by the system.

#### 3.2.2.2 Object Reuse

- a. All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation, or reallocation to a subject from the pool of unused storage objects.
- b. No information, including encrypted representations of information, produced by a prior subject's actions is to

be available to any subject that obtains access to an object that has been released back to the system.

#### 3.2.2.3 Labels

Labeling is required when a system is handling Classified data. Navy Band managed information systems handle only Unclassified data, and therefore **all** media and objects processed by the system are considered *Sensitive Unclassified* and do not require any labeling. (SECNAVINST 5239.3A designates Sensitive Unclassified as the lowest classification for all data handled by a DON system).

#### 3.2.2.4 Mandatory Access Control

Mandatory Access Control is not required for Mission Assurance Category III, and therefore does not apply to Navy Band systems.

#### 3.2.2.5 Identification and Authentication

- a The system shall require users to identify themselves to it before beginning to perform any other actions that the system is expected to mediate.
- b. The system shall use a protected mechanism (e.g., passwords, Common Access Card) to authenticate the user's identity.
- c. Authentication data shall be protected so that it cannot be accessed by any unauthorized user.
- d. The system shall be able to enforce individual accountability by providing the capability to uniquely identify each individual system user.
- e. The system shall also provide the capability of associating this identity with all auditable actions taken by that individual.
- f. The unique identification shall be the basis for validating messages.

#### 3.2.2.6 Security Audit

- a. An audit trail of security sensitive events shall be created, maintained, and protected from modification or unauthorized access or destruction by the system documenting a history of information system use.
- b. Audit records shall be reviewed on a periodic basis, as determined by the IAM in order to detect anomalies and ensure timely investigation to prevent compromise.
- c. Audit records shall be protected so that read access is limited to authorized individuals knowledgeable of the daily operations and capable of detecting anomalous events.
- d. The audit trail shall be of sufficient detail to reconstruct events in determining the cause or magnitude of compromise should security violation or malfunction occur. The audit trail will document user activity sufficiently to ensure user actions are controlled and open to scrutiny.
- e. The audit trail will document the identity of each person and device having access to the information system, use of identification and authentication mechanisms, time of access, introduction of objects into a user's address space (e.g., file open, program initiation), deletions of objects, actions taken by computer operators and system administrators and/or information assurance officers, and other security relevant events which might modify, bypass, or negate safeguards controlled by the information system.
- f. The information system shall be able to audit:
  - The origin of request for identification/authentication.
  - The name of the object for events that introduce an object into a user's address space and for object deletion events.
  - Both successful and unsuccessful operator identification and authentication checks.
  - Both successful and unsuccessful remote element identification and authentication checks.
  - Modifications to the system clock.
  - Successful and failed operator/element access control checks.
  - Successful and failed attempts to access authentication information.

- Attempts by unauthorized users to access system functions and data.
  - Attempts to access operator/element privileges and all attempts to modify operator/information system privileges.
  - The receipt of privileges.
  - Attempts to change or delete audit data.
- g. For each recorded event, the audit record shall identify the date and time of the event, user, type of event, and success or failure of the event.
- h. The system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.
- i. The decision to require an audit trail of user access to a stand-alone, single-user information system shall be at the discretion of the IAM.

#### 3.2.2.7 Architecture Assurance

The security features shall be maintained in a domain for their own execution that protects them from external interference or tampering (e.g., by modification of their code or data structures). The security mechanisms shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

#### 3.2.2.8 Integrity Assurance

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware, firmware, and software elements.

#### 3.2.2.9 Testing Assurance

Navy Band Information Assurance mechanisms shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

#### 3.2.2.10 Documentation

a. Defense Information Assurance Certification and Accreditation Program (DIACAP) documentation must be completed and maintained for every system processing government information. These systems must have an Interim Authority to Operate (IATO) or an Authority to Operate (ATO) granted by the Navy Operational Designated Approving Authority (ODAA) at NETWARCOM.

b. All appointments to required IA roles must be documented in writing to include assigned duties and appointment criteria

#### 3.2.2.11 Functional Integrity Protection

Modifications to security related functions of procured software destined for an information system shall be performed only by Information Assurance Staff. Developers and users shall ensure that all software which will reside on an information system is an exact copy of the master copy. Production copies of software should be generated from the master copy. Procedural and technical measures shall be used to protect the information system against malicious software. The information system shall employ mechanisms to detect the presence of malicious software.

#### 3.2.2.12 Data Integrity Protection

Protection shall be provided to prevent accidental or malicious alteration and unauthorized disclosure, destruction, or modification of data stored or processed by the system.

#### 3.2.3 Personnel Security Objectives

Navy Band is a White House Support unit and all assigned members hold proper security clearance to access any data kept on Navy Band systems, with the exception of Classified information accessed on the NMCI Classified network (SIPRNet) by means of a SIPRNet workstation in Field Support Activity spaces, or through the Navy message traffic system. The IAM must ensure that appropriate need-to know access is granted to users as required. A "least privilege" methodology shall be employed.

#### 3.2.4 Physical Security Objectives

The components, software, and equipment of the information system shall be located at installations that provide physical security controls commensurate with the requirements for the highest classification level and most restrictive category of information processed or stored by those components and equipment. The Naval District Washington Security Division is responsible for 24-hour physical security of the Washington Navy Yard. The Navy Band Security Officer ensures that Band spaces are secured during non-business hours. Each unit or office supervisor is responsible for ensuring that assigned workspaces and IS equipment are properly secured during and after work hours.

### 3.2.5 Procedural Security Objectives

- a. The Commanding Officer shall ensure that an Information Assurance Manager (IAM) is named, in writing, for the Navy Band, and that he or she receives applicable training to carry out the duties of this function. IAM will report directly to XO.
- b. The IAM shall report security incidents in accordance with DOD 5200.1-R to the Commanding Officer and, in the case of NMCI equipment, also to the regional IAM. All Navy Band personnel shall report any security incidents to the IAM or an Information Assurance Officer (IAO). Security incidents or violations include the following:
  - Suspected or confirmed malware on a system
  - Intrusion attempts and successes within the IS, such as:
    - Unauthorized users logging in with compromised passwords
    - Compromised administrative privileges, allowing the creation of and use of false user accounts.
  - Access denials, such as:
    - Incorrect password violations
    - Incorrect account/user names
    - Unauthorized access to certain files, directories, or other resources on the IS.
- c. The information system shall provide protection against accidental and malicious attempts to reduce its operational availability. Planning for rapid recovery from accidental or malicious system failure shall be documented and approved.

d. Contingency plans for the major Navy Band system groupings are as follows:

- Since Navy Band has a total of three Navy Band owned **Arrangers Workstations** and six NMCI workstations with Finale installed on them, in the event of failure of a primary system, one of the other systems could be used temporarily until the primary has been repaired or replaced. Navy Band arrangers have been instructed to regularly back up their data on CD so that work can be continued without significant interruption on another system if necessary.
- If one of the **AV Department Sound Board Controllers** becomes unusable, one of the other four laptops or tablet PC's could be used temporarily until the defective PC is repaired or replaced. It would be rare that all performing units would be performing simultaneously, and therefore at least one machine should be available.
- The Cruisers ensemble receptor controller greatly enhances the performances of this unit, but the group could still perform adequately without it, although not optimally. Maintaining a backup system for the unlikely event of a system failure is not cost effective.
- **The Recording Studio** system serves a unique function. In the event of major system failure, the Navy Band will contract for services through outside sources until it can be replaced. A maintenance contract could be written for this system that would serve as a contingency plan.
- Although the two **Archive** workstations are essential to the preservation of Navy Band recordings and historical materials, they are not critical to the day-to-day operations of the command. Therefore, loss of use for a short period of time would not severely impact the command's mission.
- In the event of local NMCI system failure, designated essential personnel can access the NMCI network remotely via Remote Access Service (RAS), or email via Outlook Web Access (OWA). Remote access to the NMCI network can only be achieved through use of an NMCI laptop with

either cellular air card or available wired connection (cable or DSL connection). Users of RAS must log on to the laptop before undocking it from the network to create a local profile on the machine. Personnel using OWA must complete mandatory training, be issued a CAC reader, and install CAC software on their personal computer prior to using the service. Essential personnel must perform these actions prior to the occurrence of such an event to ensure continuity of operations.

### 3.2.6 Security Education, Training, and Awareness Objectives

There shall be in place a security training and awareness program with training for the security needs of all persons accessing the Navy Band information systems. The program shall ensure that all persons responsible for the information system and/or information, therein, and all persons who access the information system are aware of proper operational and security-related procedures and risks. End user training should include:

- Value of computer-based information
- Computer vulnerabilities
- Basic safe computing
- Password management
- Virus prevention and detection
- Navy Band specific security procedures
- Explanation and demonstration of security mechanisms and safeguards on the IS
- Importance of being alert to suspicious/unusual activity.

All band members must be given a security briefing prior to being granted access to any Navy Band system.

This requirement is currently satisfied by a verbal briefing upon arrival at Navy Band and completion of annual mandatory DoD Information Assurance Awareness training via a Navy eLearning online course.

### 3.2.7 Operational Site Objectives

#### 3.2.7.1 Accreditation

- a. The accreditation of the information system shall be supported by this information assurance plan. A risk analysis of the information system in its operational environment and an evaluation of the security safeguards shall be conducted by the IAM, and a report shall be presented to the Commanding Officer for approval.
- b. IA policy shall be considered throughout the life cycle of the information system from the beginning of concept development through design, development, operation, and maintenance until replacement or disposal. The IAM shall ensure the security of the information system and shall apply for certification and accreditation through the Navy C & A process for any Navy Band owned system with a network or Internet connection.
- c. An Accreditation Report will be developed and maintained for all computer systems with network or Internet connectivity. This report must include the protection strategy and planned efforts to complete the certification and accreditation processes.
- d. The IAM shall ensure contractual requirements to protect classified and sensitive unclassified information are provided to contractors. Currently no Navy Band owned system processes classified or sensitive information.
- e. Mandatory statements of safeguard requirements shall be included as applicable in the acquisition and procurement specifications for the Navy Band. The statements shall be the result of an initial risk assessment, and shall specify the level of trust required under DODI 8500.2.
- f. The information system shall be certified and accredited with an assigned accreditation range, consisting of the set of security levels that may be associated with data it transmits and receives. Currently all Navy Band owned systems are operating at the Mission Assurance Category (MAC) III level, requiring protective measures commensurate with commercial best practices.

### 3.2.7.2 Management

Specific individuals must be assigned/designated in writing by the Commanding Officer/Leader to fulfill certain roles and responsibilities for executing the requirements of the IA Program. These security staff positions, which include an Information Assurance Manager (IAM) and one or more Information Assurance Officers (IAO's), are collateral duty assignments.

- a. The IAM shall implement and maintain an overall information assurance program designed to ensure compliance with DODD 8500.01E.
- b. The IAM shall ensure that periodic reviews of the security and protection of Navy Band information systems are done to ensure compliance with stated security goals.
- c. Changes affecting the security of the information system must be anticipated. Any changes to the information system or associated environment that affect the accredited safeguards or result in changes to the prescribed security requirements shall require reaccreditation. Reaccreditation shall take place before the revised system is declared operational. Minimally, the information system shall be re-accredited every 3 years, regardless of changes.
- d. No classified or sensitive unclassified data shall be introduced into the information system without designation of the classification and sensitivity of the data. Approval to enter the data shall be obtained from the data owner where applicable. Data entered into an information system must not exceed the highest approved security or sensitivity level for the system.
- e. When information systems managed by different Designated Approval Authorities (DAAs) are interfaced or networked, a memorandum of agreement (MOA) is required that addresses the accreditation requirements for each information system involved. The MOA should include description and classification of the data; clearance levels of the users; designation of the DAA who shall resolve conflicts among the DAAs; and safeguards to be implemented before interfacing the information systems. MOAs are required when one DOD component's information

system interfaces with another information system within the same DOD component or in another DOD component and when a contractor's information system interfaces with a DOD component's information system or to another contractor's information system.

- f. Necessary safeguards shall be agreed to and implemented and the information systems accredited for interconnection before they are connected to a network. Each information system shall be accredited to operate in accordance with a DAA-approved set of security safeguards.
- g. The IAM shall determine the security and protection requirements for connection of other information system to the Navy Band.
- h. All elements requesting interconnection must have received individual accreditation from their organization.

#### 3.2.7.3 DAA Role

- a. The Commanding Officer/Leader of the United States Navy Band is the Developmental Designated Approving Authority (DDAA) for the Navy Band and as such, shall accredit Navy Band information systems before connection to a network or the Internet.. The accreditation statement shall identify the required confidentiality, integrity, and availability services and constraints under which the system can operate including data sensitivity, user authorization, physical and system configuration.
- b. The DDAA shall review and approve security safeguards and issue the accreditation statement for Navy Band information systems under the DDAA's jurisdiction based on the acceptability of the security safeguards for the information system.
- c. The DDAA, through the IAM, shall ensure that all the safeguards required, as stated in the accreditation documentation, are implemented and maintained.
- d. The DDAA, through the IAM, shall ensure that data ownership is established for Navy Band information systems, to include accountability, access rights, and special handling requirements.

- e. The DDAA, through the IAM, shall identify security deficiencies and, where the deficiencies are serious enough to preclude accreditation, take action (e.g., allocate additional resource) to achieve an acceptable security level. There should be in place a risk management program to determine how much protection is required, how much exists, and the most economical means of providing the needed protection.
- f. DDAA's of information systems should be aware that connection to a network may involve additional risks because of the potential exposure of their own data to the larger community of all users of information systems in the network. In connections to adjacent information systems, the operational modes and security mechanisms of those information systems should be taken into consideration, beyond the simple fact of their accreditation.
- g. The security of each Navy Band information system remains the responsibility of the DDAA.
- h. The DDAA must appoint in writing, an Information Assurance Manager (IAM) who will act as a single focal point for all information assurance matters. Other security staff must also be appointed in writing. The DDAA must ensure that training for information assurance staff is provided.

#### 3.2.7.4 IAM Role

- a. The IAM and supporting Information Assurance Officers (IAO's) shall have the authority to enforce security policies and safeguards on all personnel having access to the information system for which the IAM has cognizance.
- b. The IAM shall report the security status of the information system, as required by the DDAA.
- c. The IAM shall review and forward to the DDAA for approval local security procedures and policies, ensure the safeguards are maintained as required, and evaluate known vulnerabilities to ascertain if additional safeguards are needed.

- d. The IAM shall ensure protective or corrective measures are sought out if a security problem exists.

#### 3.2.7.5 Mode of Operation

- a. Classified information shall not be processed on a Navy Band information system. Sensitive unclassified information shall be safeguarded at all times while in the information system. Information processed, produced, stored and/or transmitted by the information system shall be adequately protected with respect to requirements for confidentiality, integrity, and availability. All sensitive information shall be cleared from storage media, including computer hard drives, prior to disposal.
- b. The safeguarding of information and resources shall be accomplished through the continuous employment of safeguards consisting of communications security, computer security, personnel security, physical security, procedural security, and security education, training, and awareness.
- c. Sensitive unclassified information while in the information system shall be safeguarded against tampering, loss, and destruction and shall be available when needed. This is necessary to protect the DoD investment in obtaining and using information and to prevent fraud, waste, and abuse. Suggested safeguards for unclassified information are in Office of Management and Budget Circular No. A-130 and include applicable personnel, physical, administrative, and technical controls.
- d. The mix of safeguards selected for an information system that processes sensitive unclassified information shall ensure the information system meets the minimum requirements as set forth in SECNAVINST M-5239.1. These minimum requirements shall be met through automated and manual means in a cost-effective and integrated manner. An analysis shall be performed using SECNAVINST M-5239.1, "Department of the Navy Information Assurance Program, Information Assurance Manual" to identify any additional requirements over and above the set of minimum requirements.

NAVBANDINST 5239.1D  
15 Jun 2010

- e. All information systems that process or handle sensitive unclassified information and that require controlled access protection shall implement the required Controlled Access Protection security features.

## **SECTION 4**

### **RATIONALE FOR SELECTED OBJECTIVES**

#### **4.1 INTRODUCTION**

The Information Assurance (IA) objectives specified in Section 3.2 reflect the influence of several basic security concerns. Fundamentally, the specific IA objectives are all directly traceable to the General Security Goals for the Navy Band, as presented in Section 3.1. Specifically, the low-level IA objectives presented in Section 3.2 define the security controls necessary to ensure that the Navy Band is capable of satisfying the high-level goals presented in Section 3.1. However, the selection of the specific controls results from two basic considerations; namely, the need to comply with umbrella security guidance and the need to counter potential threats to the systems' correct operation.

In this section, umbrella security guidance and/or threat is cited as the rationale for a specific security objective, if the primary justification for the controls prescribed by the objective is the need to ensure compliance with a higher authority directive, regulation, or policy or as a consequence of the threat assessment. For example, a system security objective may reflect security needs outlined in a National security directive. In contrast, threat considerations are cited as the rationale for a system security objective if the controls prescribed by the objective serve to counter a specific threat to the correct operation of the system and the objective cannot be traced directly to umbrella security guidance.

It is important to note that there is significant redundancy in the umbrella security guidance that is applicable to the Navy Band. This is due to the hierarchical nature of authority within government organizations and the associated tendency of lower-level organizations to interpret and reflect the guidance of higher-level organizations within their own policies, regulations, and guidelines. As a result, even in cases where it is possible to trace a specific security objective to an established security need, it is not necessarily possible to trace that same objective to a single source of umbrella guidance. In other words, some objectives can theoretically be traced to multiple sources of umbrella guidance.

## **4.2 RATIONALE FOR SPECIFIC INFORMATION ASSURANCE OBJECTIVES**

The rationale for each of the IA objectives specified in Section 3.2 is identified in the tables below. For clarity, the format used in Section 3.2 has been maintained throughout this section.

### **4.2.1 Communications Security Objectives Rationale**

IAP Objective	Source Guidance
3.2.1	DoDI 8500.2, E2.1.51 DoDI 8500.2, E4.A5, DCSR-2

### **4.2.2 Computer Security Objectives Rationale**

#### **4.2.2.1 Access Control Objectives Rationale**

IAP Objective	Source Guidance
3.2.2.1	SECNAV m-5239.1, para. 5.5 SECNAV 5239.3B para. 7.b.(2)

#### 4.2.2.2 Object Reuse Objectives Rationale

IAP Objective	Source Guidance
3.2.2.2	DoDI 8500.2, para. 5.11.2

#### 4.2.2.3 Labels Objectives Rationale

IAP Objective	Source Guidance
3.2.2.3	DOD 5200.1-R para. C5.1.1

#### 4.2.2.4 Mandatory Access Control Objectives Rationale

IAP Objective	Source Guidance
3.2.2.4	DoDI 8500.2, E2.1.38.3

#### 4.2.2.5 Identification and Authentication Objectives Rationale

IAP Objective	Source Guidance
3.2.2.5	DoDI 8500.2, para. E.3.2.9 DoDI 8500.2, E4.A3 IATS-1, E4.A5 IAGA-1, IAIA-1

#### 4.2.2.6 Security Audit Objectives Rationale

IAP Objective	Source Guidance
3.2.2.6.	DoDI 8500.2, para. E3.3.10 DoDI 8500.2, E4.A3 ECAT-1, ECRG-1, ECTP-1, E4.A5 ECAN- 1, ECAR-2, ECWM-1

#### 4.2.2.7 Architecture Assurance Objectives Rationale

IAP Objective	Source Guidance
3.2.2.7	DoDI 8500.2, para. E2.1.24,

	E3.1.3.2, E3.3.2, E3.3.3 DoDI 8500.2, E4.A3 DCFA-1
--	---

4.2.2.8 Integrity Assurance Objectives Rationale

IAP Objective	Source Guidance
---------------	-----------------

3.2.2.8	DoDI 8500.2, E4.A3
---------	--------------------

4.2.2.9 Testing Assurance Objectives Rationale

IAP Objective	Source Guidance
3.2.2.9	DoDI 8500.2, para. 5.7.8

4.2.2.10 Documentation Objectives Rationale

IAP Objective	Source Guidance
3.2.2.11	DoDI 8500.2, para. 5.9.3, 5.9.4

4.2.2.11 Functional Integrity Protection Objectives Rationale

IAP Objective	Source Guidance
3.2.2.12	DoDI 8500.2, E4.A5 DCCS-1, DCDS-1, DCFA-1, DCII-1, DCIT-1, DCMC-1

4.2.2.12 Data Integrity Protection Objectives Rationale

IAP Objective	Source Guidance
3.2.2.13	DoDI 8500.2, E4.A5 IAKM-1, IATS-1, ECCD-1

**4.2.3 Personnel Security Objectives Rationale**

IAP Objective	Source Guidance
3.2.4	DODI 8500.2, E4.A3:ECCD-1, PRRB-1 DODI 8500.2, E4.A5:PRAS-1, PRMP-1, PRNK-1

**4.2.4 Physical Security Objectives Rationale**

IAP Objective	Source Guidance
---------------	-----------------

3.2.4	DODI 8500.2, E4.A5, PECF-1, PESL-1 SECNAV 5239.3B para. 7.b.(12)
-------	---

#### 4.2.5 Procedural Security Objectives Rationale

IAP Objective	Source Guidance
---------------	-----------------

3.2.5	DoDI 8500.2, E4.A3, DCSD-1 SECNAV 5239.3B para. 7.b.(13)
-------	--

#### 4.2.6 Security Education, Training, and Awareness Objectives Rationale

IAP Objective	Source Guidance
3.2.6	DODI 8500.2, E4.A5: PRTN-1 SECNAV 5239.3B para. 7.a

#### 4.2.7 Operational Site Objectives Rationale

##### 4.2.7.1 Accreditation Objectives Rationale

IAP Objective	Source Guidance
3.2.7.1	DODI 8500.2, para. 5.8.4, 5.9.4 SECNAVINST 5239.3B para. 4.h SECNAVINST 5239.3B para 7.e

##### 4.2.7.2 Management Objectives Rationale

IAP Objective	Source Guidance
3.2.7.2	DODI 8500.2, para. 5.8, 5.9, 5.10, 5.11, 5.12

##### 4.2.7.3 DAA Role Objectives Rationale

IAP Objective	Source Guidance
3.2.7.3	DODI 8500.2 para. 5.9  SECNAVINST 5239.3B para. 7.e

##### 4.2.7.4 IAM Role Objectives Rationale

IAP Objective	Source Guidance
3.2.7.4	DODI 8500.2 para. 5.9, E4.A5: PECS-1

##### 4.2.7.5 Security Mode of Operation Objectives Rationale

NAVBANDINST 5239.1D  
15 Jun 2010

IAP Objective	Source Guidance
3.2.7.5	DODI 8500.2 E4.A5: PECS-1 SECNAVINST 5239.3B para. 7.b SECNAVINST M-5239.1