Navy Cyber Forces

Commander's Cyber Security and Information Assurance Handbook

REVISION 2

26 February 2013

This document serves as guidance from the Navy C5I Type Commander for commanders, commanding officers, officers in charge, department heads, division officers, senior enlisted personnel and information systems technicians regarding the administration of local Information Assurance operations and guidance for the Cyber Security Inspection and Certification Program. This document does not cancel or supersede any policy set forth by competent authority and serves only to consolidate and amplify existing guidance for use as a reference and familiarization tool.

DEPARTMENT OF THE NAVY
COMMANDER
U.S. FLEET FORCES COMMAND
1562 MITSCHER AVENUE SUITE 250
NORFOLK, VA 23551-2487

3500
26 February 2013

Team,

From Cornelius Drebbel's introduction of the first navigable submarine for the English Royal Navy, centuries later, we have now mastered the art and science of undersea warfare in a way that is truly to our advantage. Likewise, when the Wright Brothers first brought us manned flight, it was only a matter of time until we mastered enough capability to bring 'air power' to the fight. Today we are faced with a similar challenge in the domain of cyberspace, a ubiquitous warfighting environment where our adversaries operate 24 x 7 x 365. As important as the arenas of air, land, sea/undersea, and space will always remain, a lack of mastery of the cyber domain could be to our peril.

Regardless of where we are in the work-up or deployment cycle, and no matter whether we are afloat or ashore, when operating on the network, we are on patrol and operating forward at the tactical edge the moment we have connected to the grid. Reality is that we do not have the luxury of accepting material shortfalls or lapses in information assurance practices, as shortfalls often translate into real and immediate operational risks to the entire network and to every unit attached.

Make no mistake; Cyber Security <u>is</u> Commanding Officer (CO) business. Just as you must understand the overall material condition of your ship, its weapons systems, and the readiness of your Sailors, you must have a firm grasp on cyber security. Know the proficiency of your network operators, the material readiness of your systems, and be sure to set clear and unambiguous directions regarding proper network behavior and responsibilities for your entire crew. Success in such a complex domain cannot be expected solely from your Administrators and Information Assurance Managers. Success will only be reached through consistent adherence to standards and a culture of accountability. The time to be concerned with cyber security is now, not just at the time you discover that your command will be inspected.

This manual provides a tool to help all COs understand cyber security, individual command readiness requirements, and expectations of the CO and crew. My responsibility is to ensure that you are given the proper tools, training and resources in order to meet the standards. Please study this manual and continue to share your questions, concerns, and recommendations. Be strong, sharp, and at the ready.

MICHELLE J. HOWARD
Deputy Commander

This page intentionally left blank

TABLE OF CONTENTS

		PAGE
FOREWORD	DEPUTY COMMANDER, U.S. FLEET FORCES COMMAND LETTER	ii
	TABLE OF CONTENTS	v
CHANGES	CHANGE HISTORY	viii
PREFACE	INTRODUCTION	ix
	PURPOSE	x
	SCOPE	x
CHAPTER 1	**INFORMATION ASSURANCE OVERVIEW**	1-1
	BACKGROUND	1-1
	WHAT IS INFORMATION ASSURANCE?	1-1
	IA AND THE NAVY	1-3
	DOCTRINE	1-4
	REMARKS	1-4
CHAPTER 2	**CYBER ORGANIZATION**	2-1
	CYBER C2 ORGANIZATION	2-1
	IA PERSONNEL WITHIN YOUR COMMAND	2-4
CHAPTER 3	**OVERVIEW OF THE CYBER SECURITY INSPECTION PROCESS**	3-1
	BACKGROUND	3-1
	DISCUSSION	3-1
	CYBER SECURITY INSPECTION AND CERTIFICATION PROGRAM (CSICP) STAGES	3-1
	CSI GRADING	3-3
CHAPTER 4	**PROGRAM ADMINISTRATION AND TRAINING**	4-1
	DISCUSSION	4-1

	REFERENCES	4-1
	REQUIREMENTS	4-1
	TRAINING OPPORTUNITIES	4-4
	IA/CND PROGRAM BINDER	4-5
	MONITORING AND ASSESSMENT	4-6
	TRAINING AND ASSISTANCE	4-7
CHAPTER 5	**NETWORK TECHNOLOGY**	5-1
	DISCUSSION	5-1
	REFERENCES	5-1
	HOST BASED SECURITY SYSTEM	5-1
	REQUIREMENTS	5-4
	TRAINING AND ASSISTANCE	5-8
CHAPTER 6	**TRADITIONAL SECURITY**	6-1
	DISCUSSION	6-1
	REFERENCES	6-1
	REQUIREMENTS	6-1
	TRAINING AND ASSISTANCE	6-4
CHAPTER 7	**OPERATIONAL BEHAVIOR**	7-1
	DISCUSSION	7-1
	REFERENCES	7-1
	KEY OPERATIONAL BEHAVIOR CONCEPTS/REQUIREMENTS	7-1
	REMARKS	7-3

LIST OF ENCLOSURES:

Enclosure (1) Information Security (INFOSEC) Checklist

Enclosure (2) Network Security Checklist

Enclosure (3) Certification & Accreditation Checklist

Enclosure (4) Cyber Security Workforce (CSWF) Checklist

Enclosure (5) Traditional Security Checklist

Enclosure (6) System Administrator Checklist: Daily

Enclosure (7) System Administrator Checklist: Weekly

Enclosure (8) System Administrator Checklist: Monthly/Annually

Enclosure (9) System Administrator Checklist: Initial

Enclosure (10) System Administrator Checklist: As required/after Configuration changes

Enclosure (11) Cyber Zone Inspection Items

Enclosure (12) CO's Information Assurance Quick Look

Enclosure (13) Minimum Set of Perodic Reports

Enclosure (14) Example Report: Certification & Accreditation

Enclosure (15) Sample Report: Cyber Security Workforce Training

Enclosure (16) Sample Report: Information Assurance Vulnerability Management (IAVM)

Enclosure (17) Sample Report: Weekly IA Status

Enclosure (18) Sample Report: Anti-Virus

Enclosure (19) Sample Report: 8 O'Clock Report

Enclosure (20) Sample Notice: 5050 Cyber Security Inspection

APPENDIX A LIST OF REFERENCES

APPENDIX B LIST OF URLS

CHANGE HISTORY

The following Change History Log contains a record of changes made to this document.

Date Published/ Revised	Author	Section/Description of Change
28 OCT 2011	CDR William Rhea, COMCARSTRKGRU TEN N6	Original Publication
18 JAN 2012	LCDR Hezekiah Natta, Navy Cyber Forces N412	Revision 1
26 FEB 2013	CDR Cory Brummett, Navy Cyber Forces N412	Updated references and URL lists, restructured handbook into 7 chapters, revised or rewrote all content, added CSI afloat scoring overview, added HBSS overview, revised all existing enclosures, added sample 5050 Notice (Encl 21)

Document Properties

Owner: COMNAVCYBERFOR, Code N41
Editor: CDR Mark Guzzo (mark.guzzo@navy.mil)
Discrepancies: Please report any corrections or redlines to NAVCYBERFOR N41 via the sharepoint portal

PREFACE

1. Introduction. Security for a ship begins at the brow. Topside watches and Officers-of-the Deck stand watch to ensure that the ship is secured and that unauthorized personnel do not get onboard. However, shipboard security does not stop there. Escorts provide extra security for non-cleared visitors below decks. Secure areas of the ship are protected by locks and alarm systems. Entry into those spaces are controlled by cognizant authorities and visitor logs track who has been in the space. This concept of "Defense in Depth" applies equally to the ship's connection to Cyberspace. Enclave routers and firewalls stand guard at the network's perimeter to prevent unauthorized access from outside. Network security personnel, cyber policies and procedures, and automated systems such as the Host-Based Security System (HBSS) and proxy server logs all serve to monitor activity within the network's lifelines. The combination of personnel, procedures, and products provide the layered system defense required to ensure the availability, integrity and confidentiality of the data we rely on to run our ships.

a. Across the Federal Government, cyber security incidents have soared by over 600% in the last 5 years. At least 85% of cyber intrusions could have been prevented if the following four cyber security and IA practices were routinely and vigorously followed:

(1) Patching application vulnerability.

(2) Patching operating system vulnerability.

(3) Minimizing the number of users with system administrator privileges.

(4) Employ Application "white listing" to prevent unapproved programs from running on the network.

b. Continued focus on these fundamental principles will ensure success in this dynamic cyber space domain:

(1) Cyber security is serious business; requiring all hands involvement, and

(2) Commanding Officers are engaged and involved in the management, oversight and enforcement of cyber-readiness of their ships.

2. Purpose. To establish Information Assurance (IA) techniques and procedures that utilize policies for people, processes, strategy, and technology for protecting Information Technology (IT) and information. The information in this handbook is designed to equip Commanding Officers and command personnel with the background knowledge and tools needed to effectively manage shipboard IA programs and:

a. Establish guidance for successfully maintaining command level IA-Readiness requirements.

b. Provide a common reference of all Defense and tactical level IA-related doctrine.

c. Provide training and education guidance for command IA Workforce members.

3. Scope. This document is intended to provide Commanding Officers with an overview of the fundamental issues regarding the management of our networks, providing them with (and to a limited extent) guidelines they can use in day-to-day efforts for ensuring their networks can reliably support the ship's mission and resist adversaries in the virtual realm. Although designed as a CO's handbook, this information is relevant and applicable to baseline a level of understanding for all khaki leadership. Build cyber security awareness, actions, and oversight into command daily battle rhythm, and in parallel, develop the technically competent, informed, and proactive supervisors to inculcate cyber readiness down to the deckplates. Navy Cyber Forces (CYBERFOR) N41 manages this document and solicits your feedback, lessons learned, and best practices to incorporate into future editors of this document.

GRETCHEN S. HERBERT

CHAPTER 1
INFORMATION ASSURANCE OVERVIEW

1. Background. In 1996, pursuant to a congressional request, the Government Accounting Office (GAO) reviewed the extent to which DoD computer systems experience attack. The GAO analyzed the potential for further damage to DoD computer systems and challenges in securing sensitive information on its computer systems. Subsequent reports have assessed and reaffirmed key concerns pertaining to the risk to DoD and Navy computer systems:

a. DoD relies on a complex information infrastructure to design weapons, identify and track enemy targets, pay service members, mobilize reservists, and manage supplies.

b. Use of the Internet to enhance communication and information sharing has increased DoD exposure to attack, since the Internet provides unauthorized users a means to access unclassified DoD systems.

c. While only about 1 in 500 network intrusions are detected and reported, the Defense Information Systems Agency (DISA) estimates that DoD networks are attacked about 250,000 times per year.

d. Attackers have stolen, modified, and destroyed data and software, disabled protection systems to allow future unauthorized access, and shut down entire systems and networks to preclude authorized use.

e. Security breaches pose a serious risk to national security because U.S. adversaries could disrupt the national information infrastructure.

f. Security breaches cost DoD hundreds of millions of dollars annually.

g. Additional resources are required to improve computer security, update the policies that govern computer security, and increase security training for system and network administrators.

2. What is Information Assurance? The Navy defines Information Assurance (IA) as "information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality and

non-repudiation." In short, it is the effort by which we protect our information and ensure it is available where and when we need it. IA and Computer Network Defense (CND) are sometimes used interchangeably or together, while in fact they are separate concepts. CND actions focus on mitigating threats and vulnerabilities, while IA is a much broader term that encompasses user behavior, disaster recovery and system availability. Figure 1 describes the Navy's IA strategy as "defense in depth:"

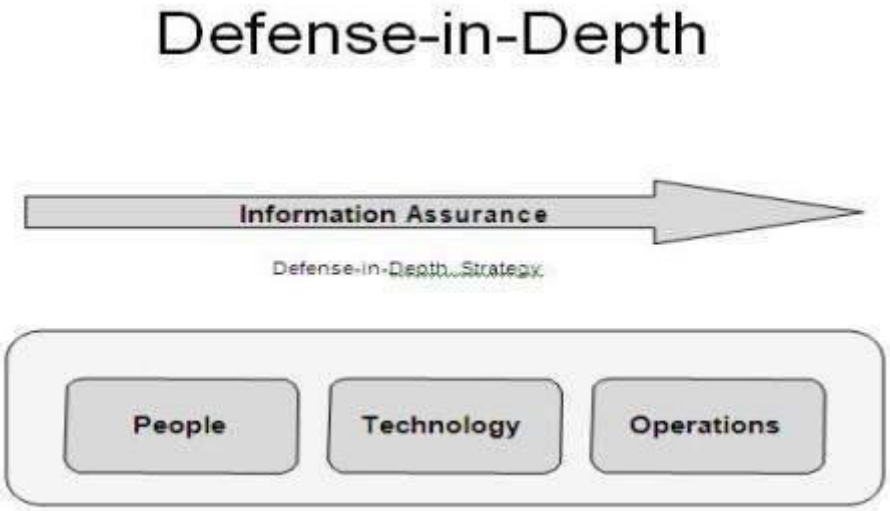

Figure 1: Defense-in-Depth

a. People. Achieving IA begins with senior level management commitment based on a clear understanding of the perceived threat. This must be followed with effective IA policies and procedures, assignment of roles and responsibilities, commitment of resources, training and personal accountability.

b. Technology. A wide range of technologies are available for ensuring IA services and for detecting intrusions. Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to deploy protection mechanisms at multiple locations to resist all classes of attack.

c. Operations. This focuses on the activities required to sustain a security posture on a daily basis, which includes Certification and Accreditation (C&A), Key Management (Communications Security (COMSEC) and the Electronic Key Management System (EKMS) program) and Readiness Assessments (Cyber Security Inspection and Certification Program (CSICP),

Board of Inspection and Survey (INSURV), or other Afloat Training Group (ATG) or Navy Type Commander (TYCOM) assessments).

3. IA Vulnerabilities. Information Assurance provides confidentiality, availability and integrity for U.S. Navy Information Systems (IS) that enable combat system operations for war fighting and Assured Command and Control (C2). An information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of information. Information Systems that exist in the U.S. Navy on ships, submarines, aircraft and expeditionary forces that utilize platform type communication systems (CS) can be considered a continuously operating forward combat system.

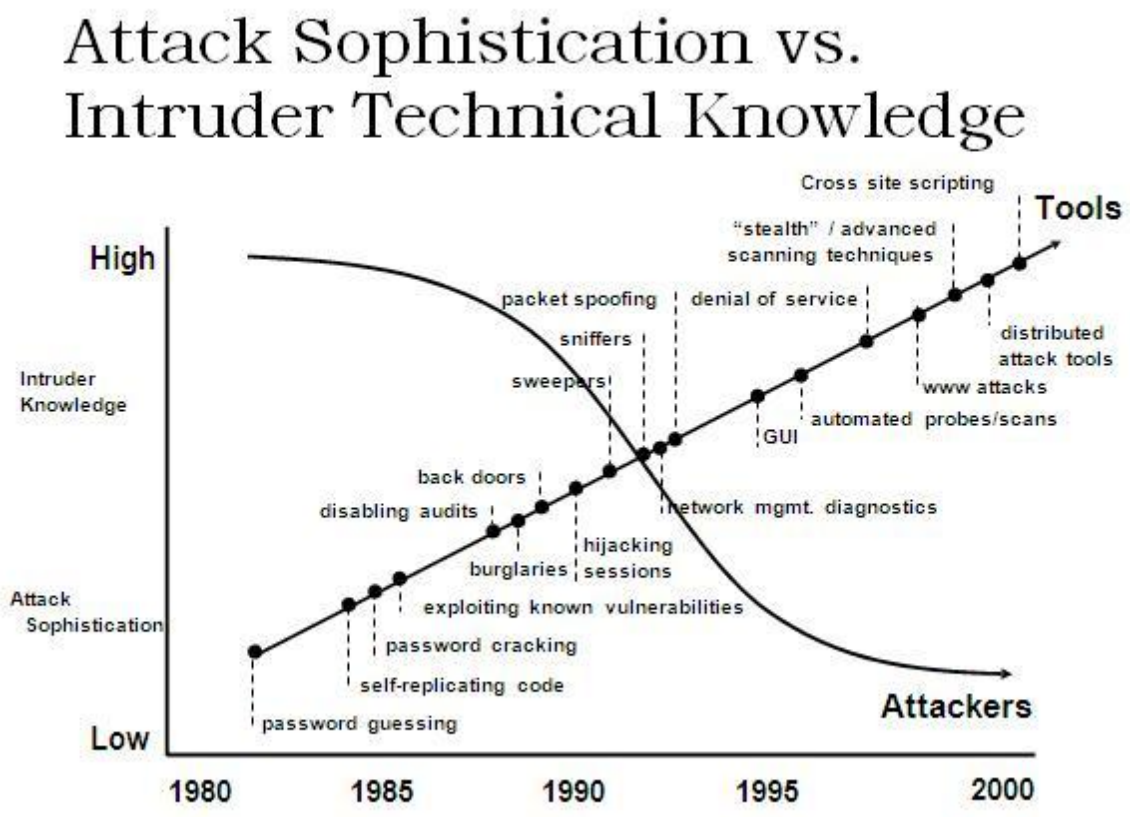

Figure 2: Improvements and proliferation of network intrusion tools allow amateur hackers to be more effective/destructive.

4. Doctrine. Reference (a) defines IA requirements for all DoD components, and reference (b) provides DoD guidance for IA implementation. For DON specifically, references (c) through (f) promulgate Navy IA, CSWF Improvement, and Information

Security policy. Numerous other instructions, directives, bulletins, and policy documents further define and codify Navy unit-level IA requirements.

5. Remarks. IA is paramount as the overarching discipline that encompasses INFOSEC, Computer Security (COMSEC), Network Security (NETSEC), and Physical Security (PHYSEC). IA incorporates the elements of each type of security into a layered defense that ensures information is readily accessible where and when needed.

CHAPTER 2
CYBER ORGANIZATION

1. Cyber C2 Organization. There are multiple commands that make up the Navy's Cyber C2 organization. Figure 3 provides an overview of these command relationships, with specific commands outlined in paragraphs below that provide direct support to afloat and ashore units.

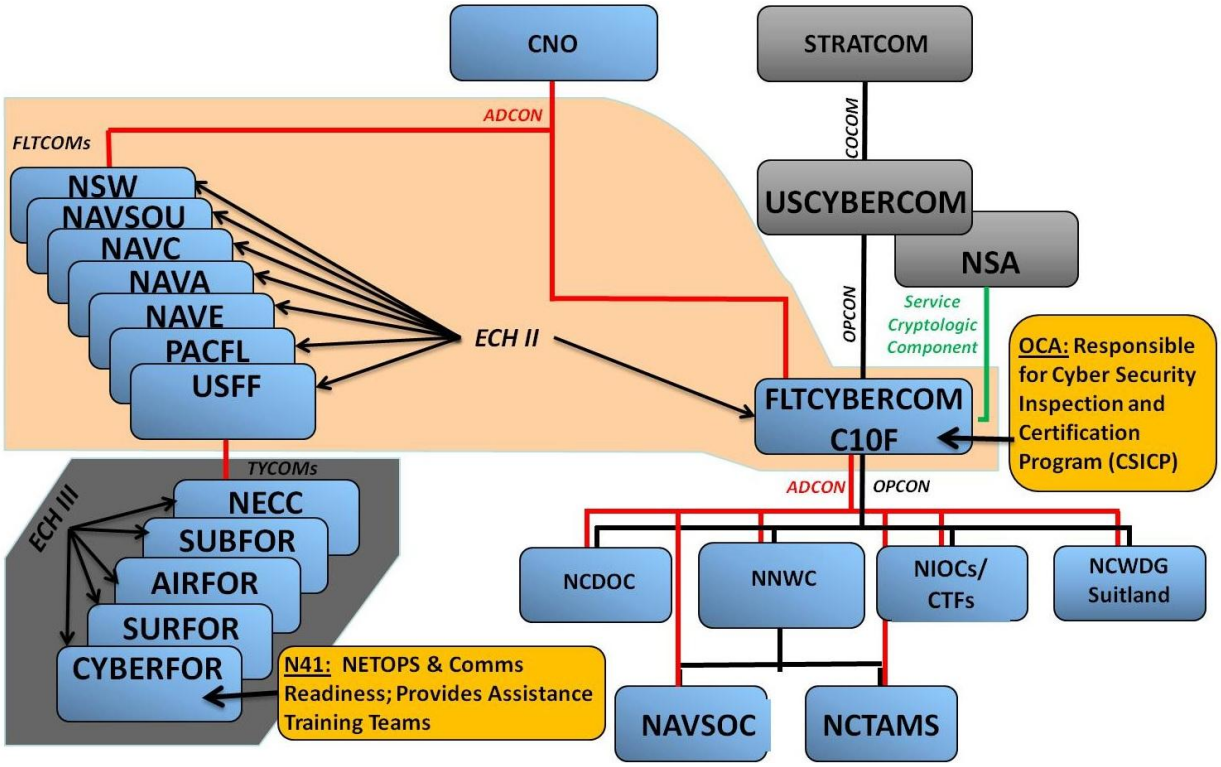

Figure 3: Cyber C2 Organization

a. **U.S. Cyber Command (USCYBERCOM).** The sub-unified cyber commander under U.S. Strategic Command (STRATCOM). USCYBERCOM centralizes command of cyberspace operations, strengthens DoD cyberspace capabilities, and integrates and bolsters DoD's cyber expertise. Consequently, USCYBERCOM improves DoD's capabilities to ensure resilient, reliable information and communication networks, counter cyberspace threats, and assure access to cyberspace. USCYBERCOM's efforts support the Armed Services' ability to confidently conduct high-tempo, effective operations as well as protect command and control systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions and attacks. **USCYBERCOM sets cyber policy for the entire DoD enterprise.**

b. **DISA.** As a Combat Support Agency, DISA provides, operates, and assures command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, National level leaders, and other mission and coalition partners across the full spectrum of operations. **DISA manages the entirety of the DoD Global Information Grid (GIG).**

c. **U.S. Fleet Cyber Command (FLTCYBERCOM/FCC)/Commander, Tenth Fleet (C10F).** C10F was reactivated 29 January 2010 as FLTCYBERCOM/C10F at Fort Meade, Maryland. As FLTCYBERCOM/FCC, it is the Naval component to USCYBERCOM, the sub-unified cyber commander. As C10F, the command provides operational support to Navy commanders worldwide, supporting information, computer, electronic warfare and space operations. In addition to joint and service reporting, the command also serves as the Navy's cryptologic commander, reporting to the Central Security Service. C10F has operational control over Navy information, computer, cryptologic, and space forces. **FLTCYBERCOM sets cyber policy for the Navy, at the direction of USCYBERCOM, and inspects Navy commands for cyber security compliance on behalf of DISA.**

d. **Program Executive Office for Command, Control, Communications, Computers and Intelligence (PEO C4I).** Provides integrated communication and information technology systems that enable Information Dominance and the command and control of maritime forces. PEO C4I acquires, fields and supports C4I systems that extend across Navy, joint and coalition platforms. This includes managing acquisition programs and projects that cover all C4I disciplines: applications, networks, communications, intelligence, surveillance and reconnaissance systems for afloat platforms and shore commands. **PEO C4I is the program manager (PM) for Navy C4I programs of record (PoRs), including the Integrated Shipboard Network System (ISNS).**

e. **Commander, Space and Naval Warfare Systems Command (SPAWAR).** As the Navy’s Information Dominance Systems Command, Space and Naval Warfare Systems Command designs, develops and deploys advanced communications and information capabilities. As the Navy’s technical lead for Command, Control, Communication, Computers and Intelligence Surveillance and Reconnaissance (C4ISR), SPAWAR provides hardware and software to connect warfighters at sea, on land and in the air, and supports the full lifecycle of product and service delivery: from the initial research and development, to acquisition and deployment,

to operations and logistics support. **SPAWAR provides the lifecycle maintenance support for PEO C4I systems.**

f. **Navy Cyber Forces (NAVCYBERFOR).** As the Navy's C5I TYCOM, NAVCYBERFOR provides relevant, resilient and effective C5I capabilities and a highly trained cyber workforce to maximize Fleet readiness and support all Naval missions through cyberspace. Responsible to U.S. Fleet Forces Command and Commander, Pacific Fleet to "man, train and equip" the Fleet for cyber operations. **NAVCYBERFOR manages Fleet readiness for C5I, and provides command training and assistance in preparation for a FLTCYBERCOM Cyber Security Inspection.**

g. **Naval Network Warfare Command (NAVNETWARCOM).** Naval Network Warfare Command's mission is to execute, under C10F Operational Control, tactical-level command and control of Navy networks and to leverage Joint space capabilities for Navy and Joint Operations. **NETWARCOM operates and defends the Navy's portion of the GIG, current Information Condition level, and provides guidance to the Fleet in the form of Computer Tasking Orders (CTOs) and Naval Tactical Directives (NTDs).**

h. **Navy Cyber Defense Operations Command (NCDOC).** NCDOC's mission is to coordinate, monitor, and oversee the defense of Navy computer networks and systems and to be responsible for accomplishing CND missions as assigned by C10F and Commander, USCYBERCOM. NCDOC Cyber Tactical Teams (CTTs) provide on-site forensic and/or analytical capabilities, and prevent loss or corruption of data/evidence that may be pertinent to a cyber incident. Furthermore, CTTs afford the ability to confirm an event based on live system analysis, and/or determine any additional data gathering actions required to facilitate an investigation. **NCDOC is the Navy's CND Service Provider (CNDSP) and provides cyber incident response, threat analysis and defense throughout the Navy.**

i. **Navy Information Operations Command (NIOC) Norfolk.** As the Navy's Center of Excellence for Information Operations (IO), NIOC Norfolk advances IO war fighting capabilities for Naval and Joint Forces by providing operationally focused training and planning support; developing doctrine, tactics, techniques, and procedures; advocating requirements in support of future effects-based warfare; and managing functional data for IO. NIOC Norfolk is home to the Navy Blue Team (NBT) and Red Team, acts as the OPSEC Support Element for the Navy, and is the parent command to NIOC San Diego (home to the West Coast's Blue Team/Red Team elements), NIOC Whidbey Island and Navy

Information Operations Detachment Groton. **NIOC Norfolk/San Diego Blue Team elements assess a command's operational behavior (via onsite network vulnerability scans) in support of the CSICP.**

2. IA personnel within your command. Reference (e), the DON Information Assurance Workforce Management Manual, outlines the IA workforce structure. Figure 4 provides a snapshot of IA duties within the workforce. Designated Accrediting Authority (DAA), Information Assurance Manager (IAM), Information Assurance Officer (IAO) and Information Assurance Technician (IAT) functions are replicated within each unit and are described in greater detail below, with verbiage directly from reference (e). Information Assurance System Architecture and Engineering (IASAE) functions remain with PEO C4I and SPAWAR for programs of record. CNDSP functions reside with NCDOC, and C&A functions reside with FLTCYBERCOM Office of Operational Designated Accrediting Authority (ODAA).

Designated Accrediting Authority (DAA) Functions	**Information Assurance Management (IAM) Levels I, II, III**	**Information Assurance Technical (IAT) Levels I, II, III**
Authorize connection/testing Accredit System Authorize IA Controls Accept Risk	Oversee configuration testing Oversee System Revalidate IA Controls Manage Risk	Manage connections/conduct testing Administer System Manage IA Controls Operate (in) Risk
Information Assurance Systems Architects and Engineers (IASAE) Level I, II, III	**Computer Network Defense Service Provider (CND SP) Functions**	**Certification and Accreditation (C&A) Functions**
Develop System Design IA Controls Engineer (out) Risk	Monitor System Assess IA Controls Detect Threat	Identify Risk/Audit Certify Recommend Accreditation

Figure 4: IA Functional Requirements, from reference (e), 1.7

a. **Commanding Officer/Deployed DAA.** The CO is ultimately responsible for the total implementation of an IA program within his or her command, including training and certification of the Cyber Security Workforce. The CO can act as the Deployed Designated Accrediting Authority (DAA) within the scope and limitations of references (e) and (s). The CO should appoint Information Assurance Manager (IAM) and Information Assurance Technicians (IAT) personnel, in writing, to manage the command's

IA program, and provide adequate oversight and command involvement in the program.

b. **Command Security Manager (CSM).** The COMSEC Manager is responsible to the CO for the proper development, implementation and enforcement of the command's personnel security posture in accordance with reference (f). The CSM will work with the IAM to develop the appropriate traditional/physical security posture of the command's information systems.

c. **Information Assurance Manager (IAM).** The IAM is responsible for ensuring the command's information system is operated, used, maintained, and disposed of in accordance with security policies and practices. The IAM should have significant IA experience and be designated in writing by the CO. Navy Enlisted Classification (NEC) 2779 (Information Systems Security Manager) is required of enlisted personnel holding this position, and must be appropriately trained and certified in accordance with reference (e). It is recommended that personnel holding the IAM position at the tactical/shipboard level be a Chief Petty Officer or above, due to the high level of trust and oversight responsibilities placed upon this position.

d. **Information Assurance Officer (IAO).** IAOs are responsible to the IAM for ensuring the appropriate operational IA posture is maintained for a command. They implement and enforce system-level IA controls in accordance with program and policy guidance. In a sense, they are the primary assistants to the IAM in implementing and enforcing IA policy. IAOs must be appointed in writing by the CO.

e. **Information Assurance Technician (IAT)/System Administrators (SA).** System Administrators may work in the computing, network, or enclave environments, and are typically of the Information Systems Technician (IT) or Cryptologic Technician (CT) ratings, but may be others provided they are properly trained and certified in per reference (e). In short, IAT/SA personnel operate and maintain a command's information systems, and are the backbone of a command's CSWF.

CHAPTER 3
OVERVIEW OF THE CYBER SECURITY INSPECTION PROCESS

1. Background. The CSICP is the Navy's process of formally inspecting afloat and ashore IA posture based on DoD, DON, DISA, and National Institute of Standards and Technology (NIST) standards. The Cyber Security Inspection (CSI) conducted by FLTCYBERCOM Office of Compliance and Assessment (OCA) for all Navy commands, follows the same format and guidelines as DISA's Command Cyber Readiness Inspection (CCRI). FCC OCA will consider a ship's Fleet Readiness Training Plan (FRTP) cycle whenever scheduling a CSI. Notification of a command CSI normally occurs 6-9 months prior. If a command has established and is maintaining a robust IA program, preparation for the CSI should cause minimal impact.

2. Discussion. Notification of the CSI schedule occurs via release of a FLTCYBERCOM Cyber Security Inspection Schedule message. Any changes to this schedule will be promulgated by message update. FLTCYBERCOM OCA will formally contact a command approximately 90 days prior to the inspection to begin coordination. NAVCYBERFOR Stage II Training and Assist Teams, partnered with NIOC Navy Blue Team personnel, are a resource available to commands to help prepare and assess cyber security compliance prior to a CSI. Stage II teams will provide command personnel training on best practices and current tactical directives, with Blue Team providing an operational behavior assessment, with report, covering all operational behavior areas that are also inspected as parto of a CSI. Outside assistance aside, a command's very best preparation for a CSI is daily vigilance and attention to detail in all areas of cyber security readiness. Enclosures (1) through (5) are designed to assist command leadership and IA personnel in preparing for a CSI. Enclosure (13) provides commanders, commanding officers and officers in charge with a range of questions to initiatate a self-assessment of IA and CND procedural compliance.

3. CSICP Stages. An overview of the three stages of the Navy's CSICP follows below:

a. Stage I: Administrative Review. This is a nominal one to 2 day review, scheduled and conducted by a command's cognizant ISIC. This review will consist of an internal review of IA and cyber security administration, leadership engagement, and personnel training and qualification. Units preparing to receive a Stage I ISIC review should review this handbook as well as NAVCYBERFOR CSICP Stage II and FLTCYBERCOM Stage III

Lessons Learned messages, and conduct a self-assessment utilizing the CSICP Stage I Checklist available via FLTCYBERCOM's CSICP portal, URL (q). Upon successful completion of a Stage I, and particularly if scheduled for a Stage III CSI, a command will progress to a Stage II unit level Training and Assessment Visit (TAV).

b. Stage II: Unit Level TAV. This is a nominal 3 to 5 day evolution (advise and assist format) scheduled and executed by Echelon II commands. For afloat units, as well as U.S. Fleet Forces Command (USFFC), FCC and Commander Pacific Fleet (CPF) subordinate commands, a Stage II TAV is conducted by NAVCYBERFOR. This assessment will include a review of Stage I, plus an additional in-depth assessment of network security, physical security and all five IA facets: Administration, Training, Personnel, Operations, and Monitoring and Assessment. Upon successful completion of Stage II, a command should be better prepared to progress to the Stage III CSI, a comprehensive inspection to be scheduled and conducted by FCC, OCA.

(1) For NAVYCYBERFOR-conducted Stage II TAVs, the assessment will contain an accompanying Navy Blue Team element, resulting in an Operational Behavior "T-score" with assessment details, provided to the command and ISIC 2-3 weeks following the Blue Team assessment via classified email. In most cases the Navy Blue Team Assessment (NBTA) will be forwarded to the unit via NAVCYBERFOR, N41 (CSICP Stage II sponsor).

(2) It is important to distinguish the Blue Team's T-score, which measures operational behavior risks to the GIG, from an overall CSI score, which the NAVCYBERFOR Stage II team does not provide. Commands will not receive an overall or ship's score from a Stage II Training and Assessment Visit. Instead a command will receive a comprehensive out-brief and extensive list of findings that will allow a command to improve their IA posture, and consequently, help to prepare for an upcoming CSI.

c. Stage III: CSI. This is a nominal 5 day comprehensive graded inspection conducted by FLTCYBERCOM OCA involving all cyber security areas, specifically; leadership engagement, physical security, administration, training, network configuration, and network operations. Stage III inspections will result in a single grade for each classification of network inspected (Secure Internet Protocol Router Network and Non Secure Internet Protocol Router Network) that represents an

evaluation of cyber security compliance with identification of operational risks to the GIG.

d. Refer to Enclosure (21) for sample Notice 5050, preparation of shipboard IA program prior to a Stage III inspection.

4. CSI Grading. DISA's grading criteria for CCRIs was adopted by FLTCYBERCOM when standing-up CSICP Stage III Inspection teams. This overall grade, which encompasses POR findings, did not convey to unit commands the level of aptitude of their crew. While POR issues are important when assessing a command's network's overall risk to the GIG, starting in June 2012 FLTCYBERCOM developed a separate score for afloat units that grades ships based on what is controllable "inside the lifelines." Figure 5 illustrates how a Stage III CSI score may be displayed during a CSI outbrief, differentiating the Ship's Force CSI score PoR findings.

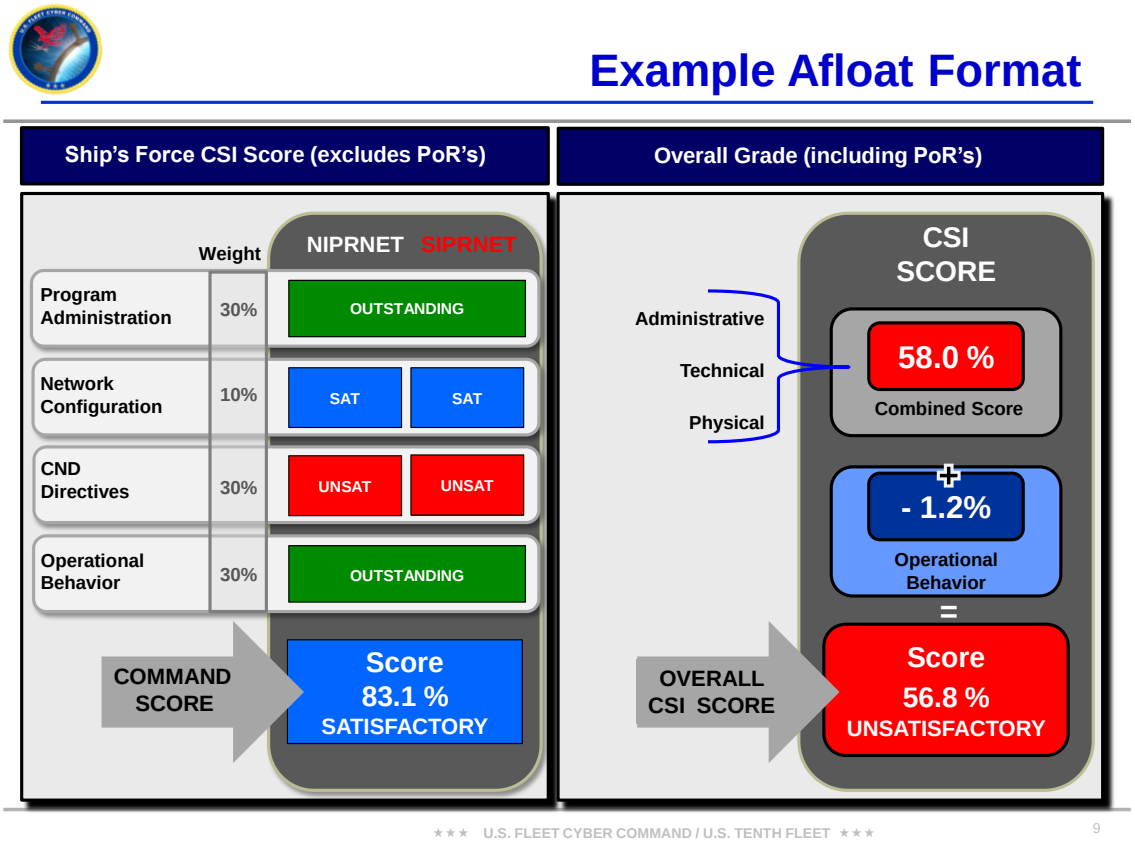

Figure 5: Revised CSI Grading Format, June 2012

a. It is important to note that the overall, traditional CCRI scoring process must still be used; excluding this score results in an incomplete risk picture. The revised afloat unit

scoring system's intent is to clearly delineate command and POR areas of responsibility, while also capturing overall risk.

b. Ship's force will be assigned a numerical score based on assessment factors that deemed to be under their control. These factors are a subset of the overall inspection criteria. This revised afloat CSI scoring methodology is further detailed in FLTCYBERCOM message, "REVISED CSI GRADING GUIDANCE," (ref. (aq)) which can be found along with the corresponding revised ship's scoring checklist and PowerPoint brief on FLTCYBERCOM OCA's UNCLAS CSICP website, URL (q). Inspection area weights below reflect relative ship's force responsibility in these areas:

(1) Program Administration (30%)

(2) Network Configuration (10%)

(3) CND Directives (30%)

(4) Operational Behavior (30%)

c. To more accurately reflect readiness, the following grading categories will be used for the ship's score:

(1) 90% or better: Outstanding. Strong cyber security environment with minimal risk to the GIG

(2) 70-89%: Satisfactory. Cyber security environment within acceptable risk to the GIG.

(3) Below 70%: Unsatisfactory. Cyber security environment is a potential risk to the GIG.

CHAPTER 4
PROGRAM ADMINISTRATION AND TRAINING

1. Discussion. Development of a command IA program begins with establishing local directives and enforcing training requirements. This is the cornerstone to your command's IA program and crucial to its success. While DoD, Secretary of the Navy and Chief of Naval Operations instructions set policy on an enterprise level, they are not designed to provide guidance at the tactical level to your specific network configuration. Thus, local policies must be created based on this existing guidance, to provide network users with a framework for network behavior and in accordance with best IA practices.

2. References. The following references will assist commands in developing local IA program policies:

a. Reference (b) is the DoD IA Implementation Guide that implements policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks. This instruction should be read and understood by all command IAM as it provides enterprise-level guidance in developing local policy.

b. Reference (e) is the DON IA Workforce Management Manual that provides guidance for managing your local CSWF and addresses training/certification requirements for members of the CSWF. Additional guidance and assistance can be obtained from Navy Cyber Forces, N1 Directorate, as the executive agent for CSWF management within the Navy.

c. References (af) and (ag) are Naval Tactical Directives (NTDs) that address requirements for incident response within the Navy enterprise and should be incorporated into a local command Incident Response Plan, discussed further in this section. Reference (r) is the DoD governing instruction, and reference (n) provides specific Navy policy instructions.

3. Requirements. The following requirements are derived from the above references and CCRI/CSI grading criteria:

a. Command leadership engagement. Enclosure (13) outlines a minimum set of periodic reports from the IAM to the Commander or CO and should be tailored at the local level. Additionally, it is recommended that commands implement Enclosures (1) through (5) as command leadership spot checks. Finally, enclosure (12)

is provided for commands to incorporate into a local zone/space inspection program. These reports and processes allow command leadership to stay engaged and informed.

b. Authority to Operate (ATO). All commands must maintain a site ATO, described in reference (h) as "granted by the [Designated Accrediting Authority] for all DoD IS to process, store or transmit information. An ATO indicates a DoD IS has adequately implemented all assigned IA controls to the point where residual risk is acceptable to the DAA. ATOs may be issued for up to 3 years." Command IAMs are trained in the C&A process and must ensure all C&A documentation is retained and tracked. Ninety (90) days prior to a site's ATO expiration, the IAM must contact the ODAA and begin the DoD Information Assurance Certification and Accreditation Program (DIACAP) review process. Additionally, each system under a POR must maintain an ATO, which in turn must be made available to sites with that system installed. Although local sites are not responsible for ensuring POR system ATOs are up to date, commands should maintain a record of all POR system ATOs.

c. Command IA Policy. Reference (b) provides specific policy requirements that must be translated into local policy, typically via a local command instruction as directed by reference (c). Specific instructions that should be included in every local IA policy are outlined as follows:

(1) Configuration Management. IAW reference (b), afloat and shore sites are required to place all DoD information systems under the control of a locally chartered Configuration Control Board (CCB). Membership in the CCB should include system administrators and IA personnel, and be designated in writing in a collateral duties notice or instruction. The CCB should meet regularly and be incorporated into the IAM's weekly schedule. Commands should retain historical documentation of CCB meetings and logs of configuration changes to the network. For afloat units, this might translate into a watch-to-watch log that tracks configuration changes to the network and is reviewed by the IAM regularly, with monthly or quarterly meetings to go over changes in procedures and keep the chain of command informed.

(2) Vulnerability Management. Per reference (b), "commands must develop a comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities in place." The vulnerability management policy should address all

vulnerabilities (not just network patches, or Information Assurance Vulnerability Management (IAVM)) that endanger the confidentiality, availability, and integrity of the information and information systems. Ensure system compliance for a newly acquired asset or network is checked before being placed on the operational network or a SOVT is signed. Command personnel must maintain communication with the program office for a given system, and refer to them for patching and baseline updates. Ensure system baselines are maintained (i.e., for ISNS, comply with SPAWAR baseline instructions in the ship's Software Version Description Document (SVDD), found via URL (m), System Operational Verification Test (SOVT) and system documentation is retained, as well as any vendor or POR-provided software kits. Provide, via local policy, specific guidance to utilize scanning software (i.e., Retina) to scan for IAVM compliance, and direct a "scan-patch-scan" methodology to find and fix vulnerabilities (refer to references (ai) and (an) for more guidance in IAVM scanning and remediation).

d. Command Incident Response and Recovery (IR&R) Policy. Networks are never 100% secure, and it is crucial that commands develop a repeatable, robust method for reporting intrusions, incidents and spillages quickly and effectively. References (ah) and (ai) provide specific guidance from the Navy's Tier 2 CNDSP, Navy Cyber Defense Operations Command (NCDOC). Additionally, reference (b) provides instructions for incident response planning. Also, URL (e) should be used and referenced in the policy for the most up-to-date direction from NCDOC. Personnel who are responsible for executing the plan must be trained and the plan must be exercised regularly in its execution. After action reports, lessons learned and all other training or incident documentation should be retained showing the plan is exercised, reviewed, and updated as appropriate.

e. Continuity Of Operations (COOP) Plan. Reference (b) provides guidance on alternate site designation, protection of back-up and restoration assets, data back-up requirements, disaster and recovery planning, and maintenance support. Development of a local COOP plan is critical for shore commands that have the ability to sustain mission essential functions in the event of a manmade or natural disaster that precludes the use of their current facilities. Afloat units meet some, but not all, measures of a COOP plan by way of data back-ups, recovery and protecting critical network infrastructure assets with uninterruptable power supply (UPS) units, ensuring these COOP measures are covered in the Planned Maintenance System (PMS) or established Standard Operating Procedures (SOPs).

f. Cyber Security Workforce Improvement Program (CS WIP). References (u) and (e) must be read and understood by all command IAMs. These references serve as the backbone for training and certifying the cyber security workforce. Local IAMs manage their CSWF program via reference (l), the Total Workforce Management System (TWMS). This online database consolidates and reports certification and training requirements for all workforce members, is viewed and tracked by Fleet leadership and staffs, and must be properly maintained at the local level to provide Fleet commanders an accurate picture. Commands must develop a local Workforce Improvement Plan (WIP) in accordance with guidance provided in reference (e). The IAM, as the CSWF Manager, must maintain and provide training plans for all workforce members, and ensure all system administrators are (a) properly trained and (b) designated in writing with signed Privilege Access Agreements (PAAs). "A," "C" and "F" school requirements are outlined for units via URL (s), available to the command's Training Officer, and should be referred to often as cyber security and information systems schools are updated regularly depending on systems installed at the command. Keep in mind that installation of updated versions of a POR system may require advanced training or a different Navy Enlisted Classification (NEC) than previously obtained. NAVCYBERFOR N1 is the Navy's agent for CSWF management and can be contacted for further information, assistance, and training.

4. Training Opportunities. Afloat units must follow FLTMPS requirements outlined within URL (s), including applicable "C" and "F" school requirements. Additional training, or emphasis on a particular Course of Instruction (COI), is provided as follows:

a. Computer Network Team Trainer (CNTT). NIOC Norfolk and NIOC San Diego periodically provide training to fleet units in tactics, techniques and procedures to harden shipboard networks against intrusions and exploitations, and provide an overview of the Navy Blue Team mission, capabilities and vulnerability assessments. Prior to commencement of a Stage I, ISICs should schedule Computer Network Team Training (CNTT) for the unit. The goal is for 60% of IT and assigned CSWF personnel to complete CNTT prior to the unit's Stage II, and 75% of IT and assigned CSWF personnel to have completed CNTT prior to the unit's Stage III. Contact NIOC Norfolk or NIOC San Diego N7 for up-to-date CNTT scheduling and quota information.

b. Host-Based Security System (HBSS). HBSS system administrators should attend the HBSS SysAdmin (Basic) school. For HBSS Version 3.0, special class convenings can be scheduled through NAVCYBERFOR N7. HBSS SysAdmin (Advanced) training has been developed by SPAWAR PMW-130, and projected to begin in January 2013. Completing both COIs will provide HBSS SysAdmins with the necessary level of understanding to utilize all of the capabilities of the HBSS suite, including built-in dashboards and security modules. HBSS is a "masters level" system and requires a commensurate level system administrator to operate, possessing Security+ certification and adequate network administration experience. Additional HBSS training, including online/virtual training, is available via the DISA IA Training Portal, URL (b).

c. Leadership Seminars and Training. Leadership-level schools, such as the Information Communications Managers Course (ICMC) and the Information System Security Manager (ISSM) course, provide valuable information pertaining to IA and CND operations. Commands should make every effort to meet these school requirements for divisional and command leadership, regardless of designation as a "critical school" in FLTMPS. It is also highly encouraged for ships to "deepen their bench" whenever possible by sending multiple leaders (including junior officers) to these schools when the operational schedule allows. Without this valuable classroom instruction, divisional and command leaders miss critical baseline training and professional networking opportunities that can assist a command in better implementing IA measures at their commands. Additionally, NAVCYBERFOR N41 and N7 conduct periodic Waterfront seminars and conferences, targeting CO/XO/Dept Head and IAM levels, that are designed to raise awareness and answer questions regarding IA requirements, successful practices, and the overall CSICP process. Further information can be found via future message traffic, ISIC correspondence, and via NAVCYBERFOR CSICP Stage II website, URL (p).

5. IA/CND Program Binder. It is highly recommended that commands develop and maintain a "program binder" that consolidates DIACAP documents, local IA policy, CSWF, IAVM and command reports, applicable DISA Security Technical Implementation Guides (STIGs), CSICP reports and any other local documents that pertain to the administration of the command's IA program.

6. Monitoring and Assessment. Reference (c) directs that all DON IA programs must be periodically evaluated for effectiveness. Evaluation must take place at all levels, from the duty System Administrator to the applicable DON oversight agency to ensure DON information systems continue to adapt to an ever-changing threat environment. The axioms "you get what you inspect, not what you expect," and "trust but verify" are also true in the realm of Information Assurance. Commands with the best IA assessment and monitoring programs are those best equipped to operate and defend in the cyber domain.

a. IA Quick Look. Enclosure (12) provides questions COs should ask their designated IAM to obtain a status report of cyber readiness for their command. The Quick Look touches on all areas of IA and can justify the implementation by management of more extensive processes necessary for maintaining the command's cyber readiness posture.

b. Periodic Reports. DoD, DON, and SECNAV IA regulations require specific periodic reports for IAVA compliance and USB scan results. Commands must develop their own IA readiness reports to ensure command leadership is continuously aware of the IA posture of their systems. Enclosure (13) lists a minimum set of reports for COs to review periodically to get a sense of the overall cyber security health of their command.

c. Spot Checks. Command IA programs encompass a wide array of auditable tasks. From various documentation requirements to include network scans to configuration management to everyday operations, there are many areas where COs, Executive Officers, IAMs and other leaders can delve into particular areas to ensure their IA program is on track. The check sheets in Enclosures (1) through (11) provide specific items to check in several key IA areas.

d. Zone Inspections. The command zone inspection program is a great place to engage the ship's INFOSEC team. In addition to looking at spaces for physical/traditional information security issues, inspectors should assess the level of knowledge of command personnel in IA security requirements. Enclosure (12) provides suggested items to be reviewed during zone inspections.

e. Self Assessments. URLs (p) and (q) offer checklists from the CSICP process that can be used as a method for command self assessment. It is recommended that commands conduct self

assessments semi-annually, concurrent with security self assessments by the CSM. As with the EKMS, periodic self assessments provide a status report to ensure a command is on course for IA compliance. Command ISICs can provide additional guidance or assistance to commands wishing to develop a comprehensive self assessment process.

7. Training and Assistance. For additional guidance, templates and tools, refer to URLs (p) and (q). Commands are encouraged to maintain regular communication with their ISIC, Platform TYCOM and Navy Cyber Forces to stay current on the latest policy changes, best practices and lessons learned. Evaluate and incorporate these lessons learned and best practices into your daily information assurance, network operations and/or information system maintenance practices.

CHAPTER 5
NETWORK TECHNOLOGY

1. Discussion. Network technology as it pertains to IA is comprised of both hardware and software solutions that work together to perform security functions on the network. Most network infrastructure devices, such as routers and switches, provide a layer of hardware security and must be maintained. Additionally, software solutions such as software-based firewalls and anti-virus programs exist to provide additional protection. This chapter discusses the references and requirements associated with network technology in accomplishing IA. In addition, an overview of the Host-Based Security System (HBSS), currently being implemented Fleet-wide, is provided.

2. References. The following references pertain to utilizing network technology to perform IA:

a. References (aj) and (ak) are tactical directives to DoD and Naval forces requiring technical implementation at the site level, and should be reviewed by command personnel to determine applicability and compliance reporting.

b. Reference (al) contains requirements for commands with approved cross domain solutions (automated process for moving data from a higher classification level to a lower classification level).

c. References (ad) and (ae) contain DoD-level guidance from DISA on the deployment and operations of the HBSS, with reference (am) providing implementation guidance specific to Naval components.

3. HBSS. DISA, in support of National Security goals established by the President, has purchased from industry a capability that will develop and deploy an automated HBSS solution to provide network administrators and security personnel with mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and information systems. Figure 6 illustrates the host-based security concept:

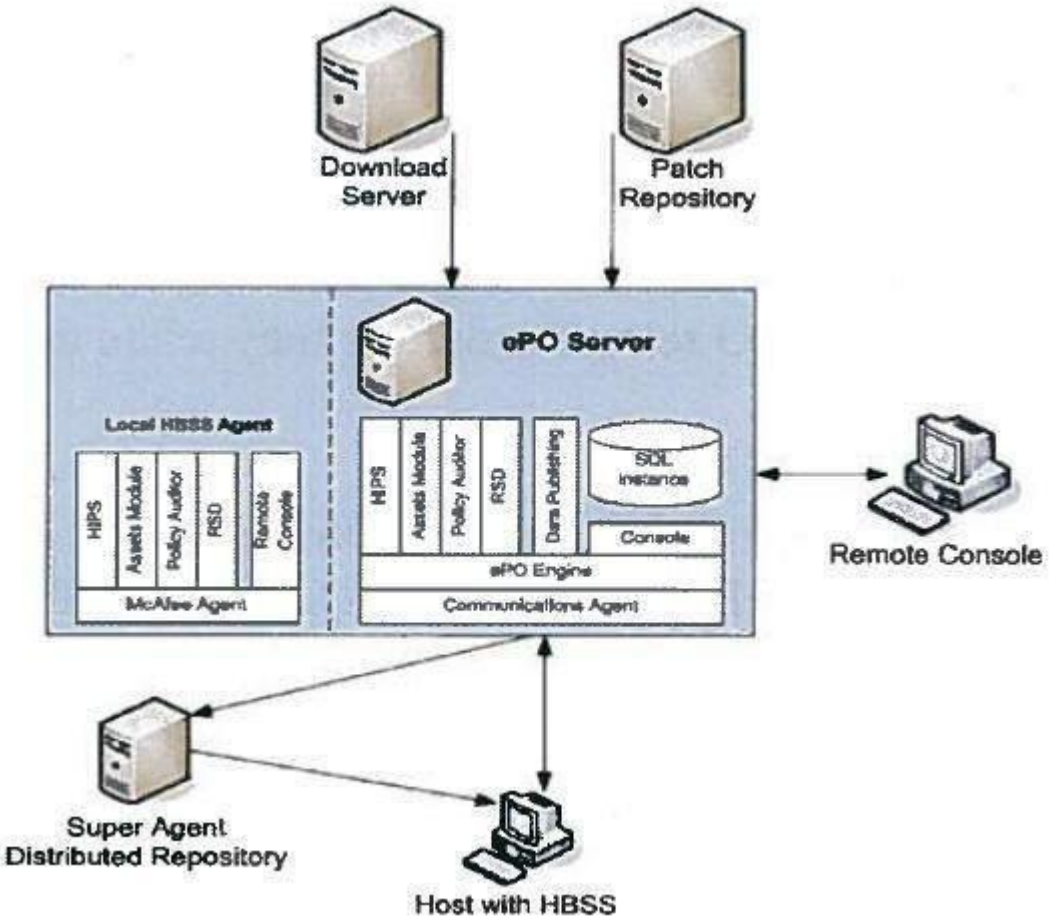

Figure 6: HBSS architecture overview from DISA HBSS CONOPS (NOTE: the Super Agent Distributed Repository is an option for sites managing thousands of assets, and not a shipboard component by design)

HBSS is a major component of a unit's IA technology pillar. Combined with Intrusion Detection Systems (IDS) at the Network Operations Center (NOC) level, these systems comprise the bulk of intrusion detection and prevention for the Fleet and represent a Defense-in-Depth strategy. SPAWAR PMW-130 is the Program Manager for the Navy's HBSS initiative, partnering with several other organizations, including DISA, to deliver this capability to Navy commands. Future capabilities planned will allow NCDOC and DISA to receive near-real time alerts and asset information at the unit level, providing redundant oversight and allowing enhanced CND command and control throughout the DoD GIG.

The governing directives pertaining to HBSS are outlined in reference (ad), which has since been officially superseded by reference (ae). Navy policy guidance on the updated

requirements of reference (ae) are outlined in reference (am). There are several HBSS requirements that all units are required to maintain per references (ad) and (ae). These are delineated in reference (am) and include the following:

a. Installation of various software security modules are required on all compatible GIG-connected systems on U.S. owned and operated DoD Secret and Unclassified networks. These modules include: McAfee Agent (MA), Host Intrusion Prevention System (HIPS), Policy Auditor, Data Loss Prevention (DLP)(which contains the Device Control Module (DCM) for control and blocking of USB devices on managed assets) and an approved Anti-Virus module, the Virus Scan Enterprise (VSE). Deployment of the Asset Baseline Module (ABM) is optional per current DISA requirements.

b. Local managers are required to configure the HBSS HIPS module to block high and medium severity signatures, and to log low severity signatures. This ensures that the HIPS component is properly preventing known intrusion attempts and notifying administrators of a suspected intrusion event. Once Secure Site status is achieved (per references (ae) and (af)), the firewall component of HIPS will be activated to provide additional network security and authorized network device connectivity.

c. Administrators must ensure <u>all</u> subnets within each enclave are actively monitored in HBSS by the Rogue System Detection (RSD) module (the only authorized excluded subnets are listed in Appendix 2 to Annex C to reference (ae)), which will notify administrators of any device connecting to RSD covered subnets that are not managed by the HBSS server (specifically, the absence of the MA). This involves knowledge of the site's specific network topology to implement properly, and the RSD module must reside on a Windows-based asset that is also being managed by the HBSS server (with all requisite end point products installed).

d. The IAM and HBSS Administrators are required to conduct daily maintenance tasks to include checking output logs, alerts and suspected rogue activity via the HBSS status "dashboard," which provides a security overview of the entire system and all connected hosts (defined as servers, desktop or laptop workstations). These tasks have been promulgated via the 3M system under a common Maintenance Index Page (MIP) series for each version of HBSS fielded to the Fleet. A dashboard entitled "Site Compliance" (installed with the system) will provide

administrators with knowledge of assets that are not compliant with reference (af).

e. It is imperative that the IAM has a firm understanding of HBSS concepts and is providing oversight over this vital security system, to include monitoring HBSS via a global reviewer account. This account allows the IAM to view events, alerts and logs in HBSS without requiring privileged access, and is also a DISA STIG directed activity.

4. Requirements. Utilizing the references outlined in paragraph 2, commands should be aware of the following network technology requirements as it pertains to Information Assurance and cyber security:

a. Password Management. For all systems, the IAM must ensure that all network device and enclave passwords are stored offline and encrypted. Passwords must not be kept in a "master list," they must instead be protected via SF-700 and stored in a GSA-approved container appropriate for the classification level of the system.

b. Information Assurance Vulnerability Management (IAVM). The IAVM process is designed to provide positive control of the vulnerability notification and corrective action process in the DoD. Commanders of Navy organizations shall comply with the IAVM process and report compliance to the appropriate combatant commander and to NCDOC via the Online Compliance Reporting System (OCRS), URL (l). Compliance is then verified by the Secure Configuration Compliance Validation Initiative (SCCVI) process (see paragraph 4.c). Commands must monitor that patches deployed have been implemented and reported. Any patches that do not install properly should be reported to the applicable system Program Management office via trouble ticket (i.e., SPAWAR's Global Distance Support Center for IT-21 systems, or the Navy's "311" Global Distance Support Center). How the system is patched depends on whether it is a POR or not. For PORs, it is a seven-step process:

(1) A commercial vendor announces a patch for a known or discovered vulnerability.

(2) DISA and USCYBERCOM analyzes the vulnerability, and if it finds the vulnerability has the potential to impact DoD operations, issues a vulnerability notice in the form of an IAVA, Bulletin (IAVB), or Technical notice (IAVT), depending on severity.

(3) NCDOC, as the Navy's CNDSP, coordinates a technical review of the vulnerability with SPAWARSYSCOM to determine applicability to Naval networks. NCDOC will then issue a tailored IAVA, IAVB or IAVT message to the Navy.

(4) The POR Program Manager (PM) tests the patch to verify it does not adversely affect system operation and then releases the patch for use. The PM then updates the OCRS site, URL (l) and the Vulnerability Remediation Asset Manager (VRAM) site, URL (k), that a patch is available for applicable affected systems.

(5) Navy commands receive an announcement via Fleet Advisory Message (FAM) or other notification from the PM that the patch is available.

(6) Navy commands apply the patch to the system. For non-PORs, the command downloads the patch directly from the vendor when directed by NCDOC, however host systems in the Fleet are PORs.

(7) Commands report compliance in OCRS, monitored by NCDOC. Once compliance has been achieved for the Navy, NCDOC reports as such to DISA and USCYBERCOM.

c. Secure Configuration Compliance Validation Initiative (SCCVI). Reference (ai) remains germane, amplified for Naval commands by reference (an), and must be read and understood by command IAMs. All commands must maintain up-to-date scanning software as instructed in the SCCVI User Guide (reference (ac)), located via SPAWAR's SAILOR 2.1 portal (URL (m)). Scans must be conducted on a monthly basis for all program of record systems (not just "ISNS COMPOSE" for afloat units) such as (but not limited to) GCCS-M, ADSI, NTCSS, Navy Cash and CND-Operating System Environment (CND-OSE, the HBSS server suite). Regardless of the software patching technology in use (i.e., IAV Manager for COMPOSE, or Windows Server Update Services, WSUS), administrators must adopt a "scan-patch-scan" methodology as described in these references to ensure patches are properly applied across the network. For all commands with POR networks (i.e., ISNS COMPOSE), the VRAM site will be utilized to store and analyze SCCVI scans, accessed via URL (k). For all others, the approved repository is the DISA-managed Vulnerability Management System (VMS), accessed via URL (n). Commands must ensure an archive of the past 90 days worth of scans exist in VRAM/VMS or are held locally.

d. Anti-Virus Updates. Anti-Virus (A/V) definitions must be kept updated to ensure proper operation. An outdated A/V client is nearly as ineffective at stopping threats to the network as not having one at all. A/V definitions must be updated every seven days. With VRAM 2.0, URL (k), A/V reports are now available as part of the scanning process.

e. HBSS. Observed compliance with references (ad) and (ae) continue to challenge the Fleet as the level of training and technical implementation varies from site to site. Commands must review these references, as well as future correspondence to Naval components in the form of Computer Tasking Orders (CTOs) or POR-based FAMs, to ensure local IAMs are current on the latest implementation guidance. HBSS is a crucial component of a command's IA posture and understanding the capabilities of this system is vital. SPAWAR HBSS Basic and Advanced training classes are available for administrators and should be utilized, as well as additional online and offline training.

f. Compliance with CTOs and FAMs. Reference (ak), USCYBERCOM CTO for Disabling Autorun, is an example of a technical CTO that continues to elude compliance even years after its release to the Fleet. Command IAMs must track and report CTO compliance to command leadership, ensuring the proper reports are made "outside the lifelines" as well, and utilize POR guidance for specified systems to reach a compliant state. For afloat units, SPAWAR releases FAMs that address specific technical tasks directed by NETWARCOM, FLTCYBERCOM, and/or USCYBERCOM and provide implementation instructions for system administrators. Compliance reporting for tactical directives, using POR guidance, cannot be stressed enough and must be a repeatable process at any command.

g. Public Key Infrastructure (PKI). Reference (ah) remains germane, and reference (ao) provides specific instructions to Naval commands regarding the implementation and enforcement of PKI requirements. In accordance with Task 2 of reference (ao), afloat units are required to enforce the digital signature policy on Unclassified workstations, regardless of whether or not they are User Based Enforcement (UBE) capable (ISNS COMPOSE Version 3.5 or higher with RAPIDS installed are UBE capable and must comply with UBE standards). Reference (ao) requires all e-mail sent with attachments and/or hyperlinks to be digitally signed. Do not use an Active Directory group policy to automate 100% enforcement, as this has the potential to cause problems in a bandwidth constrained environment. Complete details can be

found in the references. Consult POR guidance for implementation instructions.

h. Security Technical Implementation Guides (STIG). DISA publishes STIGs for common network configuration and security requirements that specify how components should be configured to minimize the risk of vulnerability exploitation on the affected network. SysAdmins should verify compliance with all STIGs that apply to their information systems components on a semi-annual basis; **POR systems must defer to PM guidance for STIG compliance and should not attempt to comply with STIG direction on their own.** Some STIGs require component modifications that are beyond ship's force capability; however, it is still incumbent upon the ship to recognize STIG non-compliance and defer these changes to the In-Service Engineering Activity (ISEA) for appropriate action.

NOTICE TO AFLOAT COMMANDS: ***Due to network configuration management requirements, do not attempt to implement STIGs without Program Manager (i.e., SPAWAR) guidance. Failure to do so can result in degraded system performance and/or loss of data.***

(1) See URL (b) for a comprehensive listing of DISA STIGs. Security Content Automation Protocol (SCAP) tools are available to automate the STIG compliance validation, however consult PoRs and command-designated Configuration Control Board (CCB) members for guidance.

(2) Failure to consult PORs on configuration changes to ensure continued system functionality before implementing a STIG configuration change may disable the information systems.

g. Universal Serial Bus (USB) Scans. Reference (ap) suspended the use of removable flash media on Navy networks and remains germane. Available for download via URL (p), the National Security Agency (NSA) developed a USB device detection tool that scans network hosts (client workstations) for unauthorized USB activity. To ensure accountability of USB usage, USB scans should be conducted weekly by System Administrators under the supervision of the IAM or an IAO. When questionable USB activity is discovered, SysAdmins must take follow-on action to identify and locate the device used and determine if incident handling and/or reporting to NCDOC is required. The Command IA Policy and account user forms should clearly state permitted and prohibited USB use and provide

appropriate enforcement authority to CSWF personnel. As with SCCVI scans, a common problem with USB scan results include:

(1) Improper administrative configuration

(2) Connectivity issues

(3) Registry keys are not routinely reset when a USB event is detected.

5. Training and Assistance. For additional guidance, templates and tools, refer to URLs (p) and (q). Commands are encouraged to maintain regular communication with their ISIC, Platform TYCOM and Navy Cyber Forces to stay current on the latest policy changes, best practices and lessons learned. Evaluate and incorporate these lessons learned and best practices into daily information assurance, network operations and/or maintenance practices.

CHAPTER 6
TRADITIONAL SECURITY

1. Discussion. The Navy's Information Security Program (ISP), involves the classification, safeguarding, transmission and destruction of classified information. Traditional security, as it relates to a command's IA program, is derived from DoD (DISA) standards and STIGs. **The command's Security Manager is responsible for these STIGs, and should be coordinating closely with the Command Information Assurance Manager to ensure compliance.** These same STIGs are what the command is graded on during a Stage III CSICP CSI. A proper traditional security program should be evident throughout the command, from outer access points (i.e., Quarterdeck check and entry) all the way down to network drops.

2. References. The following references pertain to Traditional Security and should be familiar to a command's Security Manager:

a. Reference (f) outlines the Navy's Information Security Program requirements and should be read and understood in its entirety by Command Security Managers.

b. URL (b) contains DISA STIGs. Command Security Managers must be familiar with the applicable STIGs relating to Traditional Security, specifically the following checklists: Traditional Basic, Traditional DISA, Traditional Common Computer Validation (CV), and Traditional Computer System Validation (CSV).

c. URL (t) is the Joint Personnel Adjudication System (JPAS), managed by the DoD Defense Security Service and used by Command Security Managers to verify personnel clearance information.

3. Requirements. The following requirements are derived from the above references and lessons learned from the CSICP inspection process regarding enforceable traditional security measures at Navy commands:

a. Foreign National Notification. Commands that have either foreign nationals (Naval personnel), the potential to embark foreign nationals, and/or Personnel Exchange Program (PEP)/Foreign Liaison Office (FLO) personnel assigned to their command must ensure a standard operating procedure or command instruction is in place that ensures the crew is fully aware of the limitations of foreign nationals/un-cleared U.S. personnel

as it relates to classified information and need-to-know. The SOP or instruction should identify the procedures that are required to prevent unauthorized disclosure of classified information and material.

b. Classified Storage. Although as designed, most spaces onboard ship do not meet DoD storage requirements and are not equipped with an adequate quantity of GSA-approved security containers, the command is still required to protect classified information and material. It is recommended that ships continue to follow reference (f) and at a minimum, store classified material in cabinets or cruise boxes fitted with high security locks. Shipboard classified equipment such as network computers, printers and copiers should be stored in secure spaces. If spaces do not meet vault Open Storage Standards requirements, see paragraph 3.c. below. At a minimum, access doors to these spaces should be locked when not manned by cleared U.S. personnel.

c. Vault/Open Storage Standards. Commands should identify spaces that require appropriate locks and other physical security requirements. Upon identifying deficiencies, job orders should be submitted to have appropriate issues resolved by the Intermediate Maintenance Activity (IMA) or depot during the next major availability.
* IMPORTANT NOTE: For afloat units, do not spend ship’s force manpower and OPTAR funds to correct these issues on your own. Contact your TYCOM and NAVCYBERFOR for guidance.

d. Classified Handling. Commands must follow DoD and Navy guidelines in the proper handling of classified material. Commands must develop procedures to ensure the proper protection of classified material when not in the direct control of cleared personnel. Per reference (f), use of classified coversheets and periodic training on handling of this material is required.

e. Classified Monitors and Displays. Commands must position monitors and displays in a manner that precludes inadvertent disclosure to personnel who do not have a need-to-know or an appropriate clearance. Commands can purchase privacy screens via commercial vendors for classified monitors (recommended) and face them away from entryways. Most spaces onboard ships can also resolve this by closing the access door while processing classified information.

f. Classified Meetings. A common finding from the conduct of NAVCYBERFOR CSICP Stage II TAVs is that commands have not

issued a written procedure on how to properly sanitize and conduct classified meetings in spaces that are normally not operated as secure rooms. The Command Security Manager should develop a written procedure and train the crew on how to conduct classified meetings onboard ship. The standard operating procedure or instruction should address access to the space, clearance verification and any other special circumstances such as note taking and information system requirements, etc.

g. Unauthorized Wireless Devices. All commands must ensure that not only are wireless devices not attached to their networks, but that they are not allowed into spaces that process/handle or store classified material/information. Commands, ashore and afloat, should establish a local instruction that covers use of portable electronic devices (PEDs).

h. Personnel Security. Commands must maintain a process to ensure all personnel granted access to classified information have the appropriate clearance, eligibility, signed non-disclosure agreement, and need-to-know. The approved database for processing, storing and adjudicating personnel clearances and visitor requests is the Joint Personnel Adjudication System, URL (t).

(1) Commands should have established procedures to screen all personnel for citizenship. For non-U.S. citizens assigned to the command, a Limited Access Authorization (LAA) request must be submitted if their duties involve classified information (local commanders and commanding officers typically do not have the authority to grant LAAs).

(2) Additional fields in JPAS, such as IT access levels and investigation type (NACLC, SSBI, etc.) should be completed in their entirety for all personnel, regardless of security clearance level.

(3) For access to information systems, personnel requesting access must be vetted by the command's Security Manager by signing their portion of the SAAR-N form. **Note this portion of the SAAR-N must be completed regardless of the network's classification**, as even unclassified networks may contain "sensitive but unclassified" information.

i. Security Incident Handling Procedure. Separate from the Incident Response and Recovery (IR&R) Plan discussed in Chapter Four, the Security Manager must maintain a Standard Operating

Procedure (SOP) to recognize, investigate and report information systems security incidents relating to Traditional Security. Use Chapter 12 of reference (f) as well as ISIC, local local area of responsibility (AOR) and/or Fleet Commander reporting requirements, as applicable, for guidance in developing this procedure.

4. Training and Assistance. For additional guidance, example templates and tools, refer to URLs (p) and (q). Commands are encouraged to maintain regular communication with their ISIC, Platform TYCOM and Navy Cyber Forces in order to stay current on the latest policy changes, best practices and lessons learned. Evaluate and incorporate these lessons learned and best practices into your daily IA, network operations and/or maintenance practices.

CHAPTER 7
OPERATIONAL BEHAVIOR

1. Discussion. Operational behavior can be described as day-to-day operations of the network at the user and system administrator levels. Operational behavior is a direct reflection of command culture as it relates to IA, from the Sailor on the deckplates all the way up to the CO. As the DoD (and thus the Navy) requires annual Information Assurance Awareness Training for all hands, it is clear that IA compliance is an all-hands effort. To this end, NIOC NBTs assess and evaluate operational behavior compliance during both CSICP Stage II TAVs and as part of FCC OCA's Stage III CSI.

2. References. Operational behavior is not simply a completed checklist compliance matter. It involves a combination of established tactical directives (CTOs, FAMs, Operational Orders, etc.) and best practices. Commands must utilize the OCRS, URL (l), as the Navy's repository of active Computer Tasking Orders, as well as USCYBERCOM's website, URL (o), for DoD enterprise-level directives. These directives are disseminated via record message traffic and are required to be tracked, and implemented as applicable, by the Command IAM.

3. Key Operational Behavior Concepts/Requirements. Below are key operational behavior concepts for which commands should maintain constant vigilance. By no means all-encompassing, the below list seeks to capture common findings during the CSICP process.

a. Network Configuration.

(1) Correct permissions on shared folders and files to prevent unauthorized access to PII or classified material by those that do not possess a need-to-know.

(2) Ensure proper measures are in place to restrict internet access when required (i.e., OPSEC or INFOCON).

(3) Ensure inactive user accounts are disabled or closed within 90 days of last use. Inactive administrator accounts should be closed immediately if not in use.

(4) Ensure default passwords are removed on all devices, accounts and systems. At NO TIME should a default installed

password be used operationally for ANY REASON, for ANY SYSTEM. Ensure passwords are protected via SF-700 and stored in a GSA-approved container at the appropriate classification.

b. Logs. For web proxy (i.e., Microsoft Internet Security and Acceleration (ISA) Server for the Integrated Shipboard Network System (ISNS) Common PC-based Operating System Environment (COMPOSE)), web server, Domain Name Service (DNS) and enclave/perimeter routers, event logging must be enabled and stored for a period of 90 days.

c. Human Factors.

(1) Inappropriate or unauthorized web browsing must be prevented and, if discovered, acted upon immediately. While the Fleet Network Operations Centers (NOCs) maintain a black/white list of websites that units should not be able to visit, units must also audit their local web proxy logs for unauthorized web browsing. In addition, users with privileged access (administrator rights) must not browse the internet using their administrator accounts. System administrators must be careful and use good judgment when conducting their daily routine, and use their user-level accounts for anything that doesn’t explicitly require elevated privileges to the network. It is the Command IAM’s responsibility to regularly monitor SysAdmin internet use via use of SA accounts.

(2) Prevent unauthorized devices (i.e., smart phones, music players, etc.) from connecting to the network. Flash media is prohibited by Navy policy. For commands with HBSS, the Device Configuration Module (DCM) can assist in “locking down” USB ports on workstations to prevent unauthorized devices from accessing those ports. For commands without HBSS, scanning software such as USB Detect 3.1 can be used to continuously scan for unauthorized devices. Enforcement and adherence requires constant vigilance and repeated user training, with the connection of unauthorized devices presenting a high threat factor.

(3) In addition to item (2) directly above, discovering the same device utilized on both classified and non-classified networks is a cross domain violation, as that device could have been used to move classified information to an unclassified or lower classification medium. This is a high threat factor and requires the command’s immediate attention and execution of the local Incident Response Plan.

(4) Detection of malicious software ("malware") or evidence of network intrusion (i.e., hacker penetration) is an obvious high threat factor and requires immediate execution of the Incident Response Plan.

4. Remarks. Cyber security in a readiness issue that impacts our operations in every warfare area, and failure to develop a command climate of responsible IA user behavior is a preventable vulnerability we cannot afford to ignore. Starting from the top, cyber security is a command-wide responsibility. CO, OICs and Department Heads must elevate attention, awareness, training and accountability of this issue throughout the command. Navy Cyber Forces stands ready to assist in helping commands institute a strong program and best practices.

Information Security Checklist

Date: _____

	Yes	No
1. Is the Information Assurance Manager (IAM) appointed in writing? [Command IA Policy]	___	___
2. Is the Information Assurance Officer (IAO) appointed in writing? [Command IA Policy]	___	___
3. Do the command's Secret Material Transfer Agents (SMTA) follow the procedures from the command's policy to transfer classified data to removable media? [CTO 10-25]	___	___
4. Is the command's Removable Media Representative's (RMR) list of authorized SIPRNet Media Transfer Agents (SMTAs) up to date? [CTO 10-25]	___	___
5. Do the command's SMEs and SMTAs follow the procedures from the command's policy to transfer data between networks of different classification? [CTO 10-25]	___	___
6. Does the command have an Incident Handling Policy for electronic media? [SECNAVINST M5510.36]	___	___
7. Is the IAO and LAN Division familiar with the command's policy for incident handling?	___	___
8. From a sampling of removable media onboard, are personnel properly labeling removable media? [CTO 10-25 and SECNAVINST M5510.36]	___	___
9. Has the command completed the annual inventory of all classified and unclassified ADP equipment? [Command IA Policy]	___	___
10. Does the System Administrator maintain a record of System Authorization Access Request (SAAR) forms for all command personnel and privileged users? [SECNAV INST 5239.14 (Series)]	___	___
11. Are back-ups installed in accordance with the command's Back-up and Recovery policy? [COMPOSE Back-up and Recovery Instructions]	___	___

Information Security Checklist (cont)

Date: _____

	Yes	No
12. Does the command maintain a list of approved removable storage devices? [CTO 08-08 and DISA STIG STO-ALL-030]	___	___
13. Spot check at least two files on both the the SIPRNET and NIPRNET for classification markings on the document in comparison to the content of the information. [Command Security Policy]	___	___

Commanding Officer:_____

Information Assurance Manager:_____

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER

Network Security Checklist

DATE: _____

	Yes	No
1. Is the command's IAVM Compliance greater than or equal to 90%? [Command IA Policy]	___	___
2. Does the anti-virus signature file age exceed seven days? [Command IA Policy]	___	___
3. Is the anti-virus software scheduled to scan at least weekly? [Command IA Policy]	___	___
4. Is the command in accordance with current INFOCON requirements? [ALCOM 178-08]	___	___
5. Do passwords meet minimum complexity and password age requirements? [ALCOM 178-08]	___	___
6. Are default passwords on all network components (i.e., servers, switches, workstations) changed from manufacturer passwords? [DISA STIG NET0240]	___	___
7. When logging onto the SIPRNET and NIPRNET does a DoD login banner appear? [CTO 08-008A]	___	___
8. Review the last weekly USB Detect scan log. Are anomalies investigated promptly and remedied? [Command IA Policy]	___	___
9. Are SCCVI scans uploaded to VRAM by the 20th day of the month? [CTO 08-005] **Afloat units only	___	___
10. Does the IAO ensure accounts for personnel who have transferred are removed, and for personnel who have not accessed their account in greater than 30 days are disabled? [Command IA Policy]	___	___
11. Are all back-ups verified through restoration of one or more files? [Command IA Policy]	___	___
12. Has the HBSS HIPS Admin password been changed from the default password? [DISA STIG H36140]	___	___

Network Security Checklist (cont)

DATE: _____

	Yes	No
13. Does the HBSS HIPS User Interface Admin password meet password complexity requirements? [DISA STIG H36160]	___	___
14. Is the HBSS ePO component in the enforcement mode? [DISA STIG H35500]	___	___

Commanding Officer:_____

Information Assurance Manager:_____

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER

Certification & Accreditation Checklist

DATE: _____

	Yes	No
1. Spot Check the command's binder of current Authority to Operate (ATO) documents. Are there expired ATOs?	___	___
2. Spot Check the command's binder of current System Security Authorization Agreement (SSAA) documents. Is the binder up-to-date for removed systems or newly-installed systems?	___	___
3. Is the drawing of the command's network topology current? [DISA STIG NET0090]	___	___
4. Spot check a command's workstation for applications that are not on the current copy of the Baseline Allowance Control (BAC) list. Are there applications present not on the approved BAC?	___	___
5. Review the last annual Information System Self Inspection. Are any of the discrepancies still outstanding?	___	___

Commanding Officer:_____

Information Assurance Manager:_____

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER

Cyber Security Workforce Checklist

DATE: _____

	Yes	No
1. Do the IAO, LAN Administrator and other members of LAN Division have an Online Compliance Reporting System account? [Command IA Policy]	___	___
2. Do the IAO, LAN Administrator and other members of LAN Division have an VRAM account? [Command IA Policy]	___	___
3. Do the IAO and LAN Administrator have a TWMS account? [NTD 02-09]	___	___
4. Are the CSWF personnel listed in TWMS? [NTD 02-09]	___	___
5. Do the IAO, LAN Administrator and other members of LAN Division have a SAILOR 2.1 account? [Command IA Policy]		
6. Do members of the CSWF have required certifications? [DoD 8570-01M]	___	___
7. Have all members of the command completed the current DoD Annual Information Assurance Awareness Training in NKO/e-Learning? [Command IA Policy]	___	___
8. Does the command have a training plan in place for CSWF personnel? [DoD 8570-01M]	___	___

Commanding Officer:_____

Information Assurance Manager:_____

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER

Traditional Security Checklist
(To be completed by the Command Security Manager)

DATE: _____

	Yes	No
1. Does the command have a command security instruction? [SECNAV Manual 5510.36]	___	___
2. Are the Command Security Manager (CSM) and Top Secret Control Officer (TSCO) appointed in writing by the CO? [SECNAV M-5510.36]	___	___
3. In observation of the quarterdeck watch(es), does the ship verify the credentials of non-ship force personnel at every request for access, and escort personnel who do not meet clearance requirements? [SECNAV M-5510.30]	___	___
4. Has the command completed an annual security self inspection and corrected the discrepancies (if noted) from the previous self inspection? [SECNAV M-5510.36]	___	___
5. Have space certification letters been signed for all areas where classified information is processed or stored? [SECNAV-M 5510.36]	___	___

Commanding Officer:_____

Information Assurance Manager:_____

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE COMMANDING OFFICER

System Administrator Checklist: Daily

1. Review Audit Logs.

   Tasks

   - ☐ Check application log for warning and error messages for service errors, application or database errors and unauthorized application installs.
   - ☐ Check security log for warning and error messages for invalid logons, unauthorized user creating, opening or deleting files.
   - ☐ Check system log for warning and error messages for hardware and network failures.
   - ☐ Check web/database/application logs for warning and error messages.
   - ☐ Check directory services log on domain controllers.
   - ☐ Report suspicious activity to IAO/IAM.

   Reference – COMPOSE system documentation

   Tools – Windows Event Viewer

2. Perform/Verify Daily Incremental Back-up.

   Tasks

   - ☐ Run and/or verify successful back-up of system and data files.
   - ☐ Run and/or verify successful back-up of Active Directory files.

   Reference - COMPOSE Back-up and Recovery Instructions

   Tools - Windows Back-up Tool
   Veritas Back-up Software

3. Track/Monitor System Performance and Activity.

   Tasks

   - ☐ Check for memory usage.
   - ☐ Check for system paging.
   - ☐ Check CPU usage.

   Reference - www.Microsoft.com - Monitoring Server performance.

   Tools – Microsoft Management Console
   Performance Log and Alerts

System Administrator Checklist: Daily (cont.)

Task Manager
System Monitor
Microsoft Operations Manager

4. Check Free Hard Drive Space.

Tasks

- ☐ Check all drives for adequate free space.
- ☐ Take appropriate action as specified by site's Standard Operating Procedures.

Reference - www.Microsoft.com - Monitoring Server performance.

Tools – Disk Defragmenter
Disk Management
Disk Quotas

5. Physical Checks of System.

Tasks

- ☐ Visually check the equipment for amber lights, alarms, etc.
- ☐ Take appropriate action as specified by site's Standard Operating Procedures.

6. Tactical Directives Review.

Tasks

- ☐ Go to applicable websites to review for new tactical directives:
  - o CTOs
  - o NTDs
  - o FAMs
  - o FRAGOs.
- ☐ Report applicable directives to IAM for action.

System Administrator:_____

Date:_____

System Administrator Checklist: Weekly

1. Review ISA Logs.

   Tasks

   - ☐ Check ISA/PROXY logs.

   Reference – Command IA Policy

2. Review DHCP Logs.

   Tasks

   - ☐ Review DHCP logs on each Domain Controller in the C: winnt\system32\dhcp folder.

   Reference - Command IA Policy

3. Archive Audit Logs.

   Tasks

   - ☐ Archive audit logs to a media device with one year retention.

   Reference – System Documentation

4. Perform/Verify Full Back-ups.

   Tasks

   - ☐ Run and/or verify successful back-up of system and data files.
   - ☐ Run and/or verify successful back-up of Active Directory files.

   Reference – Compose Back-up and Recovery Instruction

   Tools - Windows Back-up Tool
   Veritas Back-up Software

System Administrator Checklist: Weekly (cont.)

5. Test Back-up/Restore Procedures.

   Tasks

   - ☐ Restore back-up files to a test system to verify procedures and files.

   Reference – COMPOSE Back-up and Recovery Instructions

   Tools - Windows Back-up and Recovery Tool
   Veritas Back-up Software

6. Update Anti-Virus Signature File.

   Tasks

   - ☐ Download and install current Anti-Virus signature files.

   Reference – Windows documentation

   Downloads - www.cert.mil

7. Run Virus Scan on all Hard Drives.

   Tasks

   - ☐ Scan all hard drives using current Anti-Virus signature files.

   Reference – Windows documentation

8. Check Sailor 2.1/Navy IASE Websites for Patch Information.

   Tasks

   - ☐ Check SPAWAR approved websites to ensure correct version of scanning tools is being used.
   - ☐ Check SPAWAR approved websites for new vulnerability information including patches and hot fixes.

   Reference – SCCVI User Guide

   Downloads - http://iase.disa.mil - DoD Patch Repository
   www.cert.mil.

System Administrator Checklist: Weekly (cont.)

9. Compare System Configuration Files Against a Baseline for Changes.

Tasks

- ☐ Compare system configuration files against the baseline for:
  - All Servers
  - Random selection of five workstations/week
- ☐ Compare application executables against the baseline.
  - All Servers
  - Random selection of five workstations/week

Reference – Software Version Description Document (SVDD)

10. Run File System Integrity Diagnostics.

Tasks

- ☐ Run diagnostic tools to detect any system problems.

Reference - www.microsoft.com - Managing Disks and Volumes

Tools – Disk Defragmenter
Error-checking tool
Device Manager

11. Perform SIPR/NIPR USB Scan.

Tasks

- ☐ Scan all nodes for evidence of USB device insertion using the USB Detect Program.

12. Perform Server Clock/Time Synchronization.

Tasks

- ☐ Synchronize system clock with master server.

Reference - http://www.microsoft.com - Windows Time Service

Tools – Windows Time Service

System Administrator Checklist: Weekly (cont.)

13. Check for Unnecessary Services.

    Tasks

    - ☐ Check system services for any unnecessary services running.

    Reference – Windows documentation

System Administrator:_____

Date:_____

System Administrator Checklist: Monthly

1. Perform Self-Assessment Security Review.

Tasks

- ☐ Review technology checklist for any changes.
- ☐ Run current security review tool.
- ☐ Import results into Vulnerability Management System (VMS).

Reference

http://iase.disa.mil - Security Technical Implementation Guides (STIGs)
** ships also check for Functional Area Manager (FAM) messages
https://vms.disa.mil.

Downloads

http://iase.disa.mil – DoD IA Enterprise-wide Tools and Software: Gold Disk (.mil only). **not applicable to ships**

http://iase.disa.mil – IA Subject Matter Areas: Security Technical Implementation Guides (STIGs)
** ships also reference FAMs

Tools – Windows

DISA Field Security Office (FSO) Gold Disk and Scripts.
not applicable to ships
eEye Retina Scanner.
Citadel Hercules Remediation Tool.

Tools – UNIX

DISA Field Security Office (FSO) Scripts.
eEye Retina Scanner.
Citadel Hercules Remediation Tool.

System Administrator Checklist: Monthly (cont.)

2. Verify Retina Vulnerability Scan Performed (SCCVI).

Tasks

- ☐ Verify system scanned by IAO or IAM using Retina tool to detect for vulnerabilities and upload to VRAM no later than the 20th of every month.

Downloads - http://iase.disa.mil – DoD IA Enterprise-wide Tools and Software:

SCCVI (DoD PKI cert req'd).

3. Perform Hardware/Software Inventory.

Tasks

- ☐ Review hardware and compare to inventory list.
- ☐ Review software and compare to inventory list.
- ☐ Update applicable database.

4. Verify User Account Configuration.

Tasks

- ☐ Run DumpSec tool to verify user account configuration.
- ☐ Verify and/or delete dormant accounts with IAO approval.
- ☐ Provide output to IAO team.

System Administrator Checklist: Annually

1. Change Service-Account Passwords.

Tasks

- ☐ Work with appropriate application administrator to ensure password changes for service accounts such as database accounts, application accounts and other service accounts are implemented.

Reference

http://iase.disa.mil - Security Technical Implementation Guides (STIGs)
** U.S. ships also reference applicable FAMs

2. Review Appropriate Security Technical Implementation Guides (STIGs).

Tasks

- ☐ Review appropriate STIGs which are updated semi-annually.

Reference

http://iase.disa.mil - Security Technical Implementation Guides (STIGs)

3. Review Training Requirements.

Tasks

- ☐ Review training requirements according to DoD Directive 8570.1.

Reference

WARNING TO AFLOAT COMMANDS: ***Do not attempt to implement STIGs without Program Manager (i.e., SPAWAR) guidance. Failure to do so can result in improper system performance and/or loss of data.***

http://iase.disa.mil – IA Subject Matter Areas: Policy and Guidance.

System Administrator Checklist: Initial

1. Subscribe to STIG News.

   Reference

   http://iase.disa.mil/request-mail.html.

2. Subscribe to JTF-GNO Mailings

   Reference

   ftp://ftp.cert.mil/pub/misc/subscribe.htm.

3. Establish User Accounts with the following Web-Portals:

   - Sailor 2.1 (NIPRNET/SIPRNET)
   - VRAM (NIPRNET/SIPRNET)
   - OCRS (NIPRNET)
   - VMS (NIPRNET)
   - IATS (NIPRNET)

System Administrator Checklist: As required

As Required/After Configuration Changes

1. Test Patches and Hot fixes.
2. Install Patches and Hot fixes.
3. Schedule Downtime for Reboots.
4. Apply OS upgrades and service packs.
5. Create/maintain user and groups accounts.
6. Set user and group security.
7. Subscribe to STIG News.

After System Configuration Changes:

1. Create Emergency System Recovery Data.
2. Create new system configuration baseline.
3. Document System Configuration Changes.
4. Review and update SSAA.
5. Update VMS for Asset Changes.
6. Update VMS for IAVMs.

Cyber Zone Inspection

DATE: _____

		Yes	No
1.	Does the space contain classified information processing systems?	___	___
2.	Does the area meet the requirements for the level of information being processed?		
	Controlled Access Area (CAA)	___	___
	Restricted Access Area (RAA)	___	___
	Open Secret Storage Area (OSS)	___	___
3.	Are screens for classified systems able to be viewed from outside the space?	___	___
4.	If the space is a RAA, is an access control list posted?	___	___
5.	If the space is a CAA, RAA or OSS, is it protected with a GSA-approved lock?	___	___
6.	Are information processing systems clearly labeled with their classifications?	___	___
7.	Is there a minimum of one meter separation between classified and unclassified information processing systems?	___	___

Commanding Officer: _____

Information Assurance Manager: _____

Command Security Manager: _____

CO's Information Assurance Quick Look

Asking the following questions will give command leadership a good sense of the cyber and IA readiness of the command. Command leadership should discuss these questions with the Command IAM, CSM, IAOs and lead SAs.

Ten questions to better IA Awareness:

1. Have you designated your CSM and IAM in writing, and do they have the required training for their positions?

2. Do your command security procedures provide positive access control for all spaces where classified information is stored or processed?

3. Do all of your personnel in positions of trust (IAM, Network Administrators, etc.) have the required training and certifications according to the Cyber Security Workforce (CSWF) requirements?

4. Can your IAM tell you how many computers and other IT resources are maintained at your command?

5. Does your IAM maintain configuration drawings of your networks?

6. Is your IAM presenting you the results of the required network scans for unauthorized USB device usage for your review?

7. Does your IAM direct monthly network scans for compliance with the Information Assurance Vulnerability Management (IAVM) program?

8. Does your IAM direct that the results of monthly scans be uploaded to the Navy's Vulnerability Remediation Asset Manager (VRAM) reporting and management system, or VMS, DISA's Vulnerability Management System, as applicable?

9. Do you review the results of the monthly scans to ensure that 1) all computers are being scanned, and 2) your overall vulnerability compliance remains above 90%?

10. Do you document equipment or network security shortfalls (equipment that is too old to be patched, PoR systems that are controlled by Program Offices) with CASREPs or other requests for outside assistance?

Minimum Set of Periodic Reports

The following represents the minimum set of reports that all commands will generate on a periodic basis. The reports listed in this enclosure do not replace any reports that are required by other official instructions or directives. All periodic and irregular reports are to be retained onboard by the IAM/IAO, with copies forwarded as required.

1. Irregular Reports

a. System Operation and Verification Testing (SOVT). Any time a network connecting system is installed, the final installation step is the completion of the SOVT. Command personnel must sign the SOVT verifying that the system operates as designed and accept responsibility. An important item of note is that system cyber security discrepancies (iaw DISA STIGs or IAVM security patches) can be noted as exceptions when the SOVT is completed. This is important, since systems are often installed with known vulnerabilities. Documenting all vulnerabilities and deviation from IAVA and STIG requirements as SOVT exceptions ensures the program office does not lose track of actions required to make cyber systems compliant with IA regulations. These noted discrepancies will not pass as Cyber Security Inspection or Command Cyber Readiness Inspection (CCRI) waivers, but will assist in command awareness of cyber security requirements and as appropriate, these findings will be attributed to PoR scoring (for ships) and not the command's or ship's force responsible grade.

b. Cyber Incident Reports. In the event that a cyber incident occurs at the command, IA personnel shall provide timely initial and regular update reports to the command team on actions taken and how the incident affects the command's IA posture and overall mission readiness.

2. Semi-annual Reports

a. Certification and Accreditation. Review the status of all command systems' Authorities to Operate (ATOs). For any ATO within 6 months of expiration, the report shall indicate what actions are being taken to ensure that all command's systems will retain their accreditation.

b. Network Configuration. Review the command's network diagrams. Drawings should be up-to-date and include any changes to the network configuration that has occurred in the previous 6 months. Accurate network diagrams are critical to successful network management and are required for ATO renewal and Cyber Security Inspections.

3. Monthly Reports

a. CSWF Training. Review the status of required IA training for all Cyber Security Workforce personnel. Additionally, all hands are required

to complete on-line IA Awareness Refresher training within the last year. Additionally, personnel in positions of trust (system administrators, command IAM/IAO, etc.) shall be certified at the required level of IA training or must have submitted waivers for completion.

b. Privileged User Training. Review the list of personnel who have been granted system administrator rights on the network. These personnel shall have a valid need for this access, will be designated in writing, and shall have the appropriate level of training and qualification in accordance with CSWF guidance.

4. Bi-weekly Reports

a. IAVM Reports. Review the status of the command's compliance with all identified IA vulnerabilities. This report will include results of periodic SCCVI network scans and show the percentage of command's computers that have been updated with all available patches. In reviewing the IAVM report, special attention shall be taken to ensure that all computers on the network are being scanned, and that missing patches are being tracked and individual computers are being updated as necessary.

5. Weekly Reports

a. Weekly IA Status Report. The IAM shall provide a report that gives an overview of the command's IA posture. Although less detailed than the other individual reports in this section, the IA Status Report provides leadership with all the data required to ensure that the command is maintaining a proper level of cyber readiness.

b. Anti-virus Signatures. New anti-virus signatures are typically released weekly. Network records shall be reviewed to ensure that the signature updates have been applied to all computers. As with IAVM reports, attention shall be given to the number of computers reported as compared to the number actually on the network, and all discrepancies addressed.

6. Daily Reports

a. USB Scans. Networks shall be scanned daily for unauthorized USB device usage. The results of these scans should be a part of regular daily reports. Once again, the number of computers scanned shall closely match the number of computers on the network. If any unauthorized

activity is detected, follow-up actions will also be reported and action taken in accordance with the ship's policy for proper use of USB devices.

7. Sample Reports. The following pages provide templates for the periodic reports delineated above. Existing report formats need not be changed as long as they provide the same information as the reports below.

Sample Report - Certification & Accreditation

USS [Ship name] Certification and Accreditation Report
(Semiannual)

Date:_____

System Name	Last ATO Date	ATO Exp Date	Next Action	Due Date	Action Status
ISNS Compose 3.0.0.0 (NIPRNet)	May 2009	May 2012	Submit C&A Package to ODAA	Dec 2011	Assembling package
ISNS Compose 3.0.0.0 (SIPRNet)	Jun 2009	Jun 2012	Schedule vulnerability assessment	Nov 2011	Contacting NIOC Blue Team to schedule
Other systems					

IAM: _____ **Date:** _____

CSO: _____ **Date:** _____

XO: _____ **Date:** _____

Sample Report - CSWF Training

USS [Ship name] CSWF Training Report
(Monthly)

Date:_____

IA Qualification

Name	Position	Rqd IA Lvl	Qual Status	Due Date	Waiver Req Status
ITCS Jones	IAM	IAM	90% compl	Dec 2011	N/A
IT2 Kelly	Sys Admin	IAT Level II	50% compl	Mar 2012	6-mo extension approved by ODAA from Sep 2011

2735-2791 NEC Conversion

Name	ADNS CBT	ISNS CBT	Security+	MS 290	MS 291	Due Date	Pkg Submitted
IT2 Kelly	20Jul11	24Jul11	12May11	13Aug11	3Sep11	30Sep12	10Sep11
IT3 George	15Sep11	25Sep11	2Oct11	15Oct11	2Nov11	30Sep12	--

IAM: _____ **Date:** _____

CSO: _____ **Date:** _____

XO: _____ **Date:** _____

Sample Report - IAVM

USS [Ship name] IAVM Report
(Monthly)

Date:_____

System	No. of Computers on System	No. of Computers Scanned	Total Available Patches	No. of Patches Applied	No. of Computers Below 90%	Average Compliance %
NIPR COMPOSE	55	50	354	350	4	95%
NCTSS	1	1	XX	XX	XX	XX
Navy Cash						

IAM: _____ **Date:** _____

CSO: _____ **Date:** _____

XO: _____ **Date:** _____

Sample Report - Weekly IA Status

USS [Ship Name] Weekly IA Status Report

Date: _____

	NIPR	SIPR	CENTRIXS	(Others)
# of Servers				
# of Workstations				
Information Assurance Vulnerability Management (IAVM) Scans				
# Scanned				
Last Scan				
% Compliance				
Last VRAM Upload				
Antivirus				
Definition Date				
Last Scan				
# Scanned				
Viruses Found				
USB Detect				
Last Scan				
# Scanned				
# Authorized Use				
# Unauthorized Use				
Backups				
Completed Date				
Tested Date				

Sample Report - Weekly IA Status (cont.)

Cyber Security Work Force (CSWF)			
	# Required	**# Completed**	**# in Total Workforce Management System (TWMS) Database**
Current			
90-Day Projection			
120-Day Projection			

Authorized DFS		**Scheduled Maint**	
Privileged Users		**Locked Accounts**	

IAM: _____ **Date:** _____

CSO: _____ **Date:** _____

XO: _____ **Date:** _____

Sample Report – Anti-virus

USS [Ship name] Anti-Virus Report
(Weekly)

Date:_____

System	No. of Computers on System	AV Def Date	Last Scan Date	No. of Computers Scanned	No. of Computers Out of Date	No. of Threats Found
NIPR COMPOSE	55	20Oct11	24Oct11	52	3	0
SIPR COMPOSE	XX					

IAM: _____ **Date:** _____

CSO: _____ **Date:** _____

XO: _____ **Date:** _____

Sample Report - USB Scan

USS [Ship name] USB Scan Report
(Daily)

Date:_____

USB Detect Version: 3.1

System	No. of Computers on System	No. of Computers Scanned	Last Scan Date	No. of Instances Found	Action Taken
NIPR COMPOSE	55	48	24Oct11	1	Device identified & confiscated. Individual account locked pending further action.
SIPR COMPOSE					

IAM: _____ **Date:** _____

CSO: _____ **Date:** _____

XO: _____ **Date:** _____

Sample Report - 8 or 12 O'Clock Report

USS [Ship name]
Cyber Security 8 O'clock Report
(Daily)

Date:_____

Cyber Reports	**Periodicity**	**Last Date Completed**	**Discrepancies Noted (Y/N)**	**Discrepancies Reported (Y/N)**	**Action Officer (IAM, COMMO, CSO, CO)**
USB Scan Report	Daily				
Anti-Virus Report	Weekly				
IA Status Report	Weekly				
IAVM Report	Monthly				
CSWF Training Report	Monthly				
Certification and Accreditation Report	Semi Annual				
Cyber Spot Checks	**Date Scheduled**	**Last Date Completed**	**Discrepancies Noted (Y/N)**	**Discrepancies Reported (Y/N)**	**Action Officer (IAM, COMMO, CSO, CO)**
Certification and Accreditation					
Cross Domain Solution (as applicable)					
CSWF					
Information Security					
Network Security					
Physical Security					
Cyber Zone Inspection					

IAM: _____ **COMMO:**_____ **CSO:** _____ **XO:** _____

SAMPLE NOTICE 5050 – CYBER SECURITY INSPECTION

USS ALWAYSREADY (CVN 99) NOTICE 5050

Subj: SCHEDULE OF EVENTS AND RESPONSIBILITIES FOR CYBER SECURITY INSPECTION AND CERTIFICATION PROGRAM (CSICP) STAGE III INSPECTION

Encl: (1) Inspection Schedule
(2) Pre-Inspection Checklist

1. Purpose. To provide information, assign responsibilities and ensure effective coordination for CSICP Stage III inspection to be conducted from 24-30 August 2012.

2. Scope. Commander, Fleet Cyber Command will conduct an inspection of USS NEVERSAIL from 24-30 August 2012. This is the final stage in a three-stage Cyber Security Inspection and Certification Program (CSICP) process that will ensure the health and security of Navy networks and connected combat systems. CSICP Stage III is an inspection to be conducted by Fleet Cyber Command Office of Compliance and Assessment (OCA) encompassing all administrative, technical Information Assurance, Traditional (Physical) Security programs and policies. Successful completion will result in a certification report by Fleet Cyber Command to U.S. Cyber Command that USS NEVERSAIL has completed its CSICP Stage III Command Cyber Readiness Inspection (CCRI).

3. Action

a. CCRI Coordinator

(1) Ensure proper coordination and execution of CSICP Stage III.

(2) Advise the Executive Officer and Commanding Officer of all matters relating to the assessment.

(3) Host daily Hot Wash with inspection team, Combat Systems Department representatives, Security Manager and others as required.

b. Operations Officer. Ensure the event is annotated on the Green Sheet and coordinated with other events.

c. Combat Systems Officer

(1) Assign Combat Systems Information Officer as the primary point of contact for all internal and external planning and execution of CSICP Stage III.

(2) Provide oversight for all internal and external planning and execution of CSICP Stage III.

(3) Provide audiovisual support for CSICP Stage III in-brief.

(4) Provide work area for inspectors and access to required information technology systems.

(5) Coordinate and consolidate the CSICP Stage III After Action Plan (AAP) for Commanding Officer and Executive Officer.

d. Combat Systems Information Officer (CSIO)

(1) Assign team leads to support all aspects of the CSICP Stage III technical and administrative information assurance portion of the inspection.

(2) Schedule Commanding Officer in-brief and out-brief by the inspection team.

(3) Prepare and deliver USS ALWAYSREADY in-brief for the inspection team.

(4) Provide a list of inspection team members with security clearance information to the Command Security Manager, Security Officer (and AIMD Officer or others as appropropriate) to facilitate command access and designated parking.

(5) Provide a list of all out-brief attending personnel to TYCOM N6; coordinate JPAS Visit Request with cognizant Security Managers.

(6) Ensure all required documentation is prepared, and delivered electronically IAW inspection team timeline requirements, and presented to the inspection team upon arrival.

(7) Provide an After Action Plan (AAP) to the CSO following the conclusion of CSICP Stage III.

e. Security Manager

(1) Validate all visiting inspection team member security clearances via JPAS.

(2) Send JPAS Visit Request to TYCOM for all USS ALWAYSREADY out-brief attendees.

(3) Coordinate all Traditional Security requirements as determined by inspection team. Provide inspection team access to required

physical and personnel security instructions, policies and other documentation as required.

(4) Provide an AAP to the CSO following the conclusion of CSICP Stage III.

f. Security Officer

(1) Ensure validated inspection team roster with security clearance information is delivered to the (Enlisted) Quarterdeck prior to inspection team arrival.

(2) Ensure that watch standing personnel are briefed on proper identification and clearance verification procedures prior to visitor badges being issued to FCC OCA inspection team members.

(3) Reserve and prepare a space that will support physical security interviews.

g. AIMD. (Example as assigned) Provide parking signs as required for the inspection team. Post signs in Pier XX Officer parking prior to 1800 on 23 August 2012.

h. Supply Officer

(1) Reserve and prepare the Wardroom to support formal in-brief.

(2) Prepare and provide refreshments for guests during the in-brief (Note: not required).

i. Chief Engineer. In coordination with the Security Manager, facilitate installation of approved locks on all spaces that process or store classified material.

j. All Departments

(1) Department Heads or designated representatives will conduct CSI pre-inspection utilizing enclosure 2. Certify inspection results to the Intelligence Officer by e-mail before 20 August. The Intelligence Officer will consolidate results for review by the Commanding Officer on 20 August.

(2) Coordinate removal of SIPRNET workstations from all spaces not designated in writing as a Restricted Access Area or Open Storage Secret by the Security Manager no later than 19 August.

(3) Remove wireless phones from spaces that process or store classified material no later than 21 August.

(4) Provide access to spaces as required by inspection team.

3. Uniform. Navy Working Uniform.

4. The Intelligence Officer (or whomever so designated) is the point of contact for this notice.

5. Cancellation. This notice is canceled upon completion of the visit.

//s//
I. M. INCHARGE

USS ALWAYSREADY (CVN-99)
CSICP STAGE III INSPECTION
DD – DD MMM YYYY

Friday (24 Aug)

0730 FCC OCA CCRI team arrives
0900-1000 Formal in-brief w/CO/XO/IO/CSO/CSIO/ADPO/IAM (W/R 3)
1000-1700 Begin technical and administrative inspection
1100-1200 Lunch
1700-1800 HOT WASH w/IO/CSO/CSIO/ADPO/IAM (Ready Room 8)

Saturday (25 Aug)

Inspection team stands-down.

Sunday (26 Aug)

Continued stand-down.

Monday (27 Aug)

0730-1700 Continue with technical and administrative inspection
1100-1200 Lunch
1700-1800 HOT WASH w/IO/CSO/CSIO/ADPO/IAM (Ready Room 8)

Tuesday (28 Jun)

0730-1700 Continue with technical and administrative inspection
1100-1200 Lunch
1700-1800 HOT WASH w/IO/CSO/CSIO/ADPO/IAM (Ready Room 8)

Wednesday (29 Aug)

0730-1700 Continue with technical and administrative inspection
1100-1200 Lunch
1700-1800 HOT WASH w/IO/CSO/CSIO/ADPO/IAM (Ready Room 8)

Thursday (30 Aug)

0730-TBD Continue with technical and administrative inspection
TBD COMPILE ANALYSIS – Build out-brief
TBD Conduct out-brief w/CO/XO/IO/CSO/CSIO/ADPO/IAM (CNAL)
TBD FCC OCA CCRI team departs

Date: _____

MEMORANDUM

From: Department Head
To: Commanding Officer
Via: Intelligence Officer
Executive Officer

Subj: DEPARTMENTAL CCRI PRE-INSPECTION VALIDATION

1. Information Assurance/Traditional Security Checklist:

a. If SIPRNET LAN drops are present, has the space been designated in writing as a Controlled Access Area or Restricted Access Area?

b. If the space has not been designated in writing, have all SIPRNET computers been removed and drops secured by ADP (x6770)?

c. Are computers, monitors and printers labeled at the highest level of data processed?

d. Are NIPRNET/SIPRNET computers spaced at least 3 feet apart?

e. Are monitors that display classified information positioned in a manner that prevents unauthorized viewing?

f. Are USB stickers placed over USB ports?

g. Are SECRET hard drives locked in an approved GSA safe at the end of the day, if not in a controlled environment?

h. Have all wireless phones been removed from spaces that store or process classified information?

i. Are "DO NOT DISCUSS CLASSIFIED INFORMATION" phone stickers placed on non-secure phones?

2. Certification of Completion. I have spot checked X of XX spaces, including all spaces that process classified information, and have noted (*the following*, or *no*) discrepancies.

Department Head Print/Sign: _____/_____

LIST OF REFERENCES

Compiled References can also be found at Navy Cyber Forces website, URL (p), Public Documents → References → IA Handbook Reference List

(a) DODD 8500.01E, Information Assurance
(b) DODI 8500.2, Information Assurance Implementation
(c) OPNAVINST 5239.1C, Navy Information Assurance Program
(d) SECNAVINST 5239.3B, DON CIO Network Policy
(e) SECNAV M-5239.2, DON Information Assurance (IA) Workforce Management Manual
(f) SECNAV INST/MANUAL 5510.36 DON Information Security Program Manual
(g) NIST Special Publication 800-128, Configuration Management Guide for Information Systems
(h) DODI 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP)
(i) SECNAVINST 5520.3B, Criminal and Security Investigation and Related Activities within the Department of the Navy
(j) DoDD 5200.2, DoD Personnel Security Program
(k) DON DIACAP HANDBOOK V.1
(l) CJCS Instruction 6510.01F, Information Assurance (IA) and Support to Computer Network Defense (CND)
(m) DON CIO 221246Z AUG 07, DON CIO Goals
(n) SECNAVINST 5239.19, DON Computer Network Incident Response and Reporting Requirements
(o) Joint DODIIS/Cryptologic Sensitive Compartmented Information (SCI) Systems Security Standards Rev 4
(p) Naval Tactical Directive (NTD) 06-10 (ALCOM 137/10, 101721Z Sep 10), Password Requirements
(q) NAVNETWARCOM Computer Tasking Order (CTO) 08-11 (040150Z Dec 08), Implementation of Information Operations Condition (INFOCON) Level 3
(r) CJCS Manual 6510.01B, Cyber Incident Handling Program
(s) Naval Tactical Directive (NTD) 07-09 (ALCOM 103/09, 231600Z JUN 09), Implementation Instructions and Restrictions on the Deployed Designated Accrediting Authority (DAA)
(t) NIST Special Publication 800-34 Rev. 1, Contingency Planning Guide for Information Technology Systems
(u) DoD 8570.01-M CH 2, Information Assurance Workforce Improvement Program
(v) DODINST 5230.29, Security and Policy Review of DoD Information for Public Release

(w) OPNAV 5239/14 (REV 9/2011), System Authorization Access Request Navy (SAAR-N)
(x) DODINST 8520.2, Public Key Infrastructure (PKI) and Public Key (PK) Enabling
(y) INSURVINST 4730.27, Information Systems Material and Security Inspection
(z) OPNAVINST 5450.345, Mission, Functions, and Tasks of Commander, U.S. Fleet Cyber Command and Commander, U.S. Tenth Fleet
(aa) NAVSO P-5239-04, Information Systems Security Manager (ISSM) Guidebook, Module 04 INFOSEC Program Guidelines
(ab) Secure Configuration Compliance Validation Initiative (SCCVI) eEye Digital Security Retina Network Security Scanner User Guide v2.0 (SPAWARSYSCEN PAC), revised 28 September 2012
(ac) Information Communications Manager’s Course (ICMC) Student Guide (CIN: A-202-0041)
(ad) FRAGO 13 TO USCYBERCOM OPORD 05-01, Change 5 dated 20 June 2011, Deployment of Host Based Security System (HBSS) on SIPRNET
(ae) USCYBERCOM OPORD 12-1016, 21 August 2012, Host Based Security System (HBSS) Deployment and Operations
(af) Naval Tactical Directive (NTD) 11-08 (ALCOM 156/08, 032052Z Nov 08), NCDOC Electronic Spillage Response
(ag) Naval Tactical Directive (NTD) 04-06 (ALCOM 046/06, 151503Z May 06), NCDOC Incident Response Requirements
(ah) USCYBERCOM Computer Tasking Order (CTO) 07-015 (11 Dec 07), Public Key Infrastructure (PKI) Phase II
(ai) USCYBERCOM Computer Tasking Order (CTO) 08-005 (23 Apr 08), Scanning and Remediation
(aj) NAVNETWARCOM Computer Tasking Order (CTO) 08-05A (221515Z Jul 08), Standard Consent Banner and User Agreements
(ak) USCYBERCOM Computer Tasking Order (CTO) 09-002 (15 May 09), Disabling Autorun
(al) FRAGO 12 to USCYBERCOM OPORDER 05-01 (Validation of DoD and IC Cross Domain Solutions) 26 Nov 08
(am) NAVNETWARCOM Computer Tasking Order (CTO) 12-10 (021800Z Aug 12), HBSS Deployment and Sustainment
(an) NAVNETWARCOM Computer Tasking Order (CTO) 11-16 (061955Z Jul 11), Secure Configuration Compliance Validation Initiative (SCCVI) and VRAM Requirements
(ao) NAVNETWARCOM Computer Tasking Order (CTO) 09-07 (091624Z Jul 09), PKI Implementation and Enforcement

(ap) NAVNETWARCOM Computer Tasking Order (CTO) 08-08 Change 4 (170135Z Nov 08), available via SIPRNET, URL (e)
(aq) COMFLTCYBERCOM, Revised CSI Grading Guidance (U) message, DTG: 162020Z Jul 12

LIST OF URLS

(a) Navy Cyber Forces – Cyber Security Work Force UNCLAS portal
https://usff.portal.navy.mil/sites/cyberfor/cswf/default.aspx

(b) DISA Information Assurance tools
http://iase.disa.mil/tools/index.html

(c) Department of Defense (DoD) patch repository for common supported operating systems and applications (NOTE: Not for SPAWAR Programs of Record)
UNCLAS: https://patches.csd.disa.mil
GENSER: https://patches.mont2.disa.smil.mil

(d) Navy Information Security site
https://infosec.navy.mil

(e) Navy Computer Defense Operations Command (NCDOC) site
UNCLAS: https://www.ncdoc.navy.mil
GENSER: https://www.ncdoc.navy.smil.mil

(f) Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) Knowledge Service (KS)
https://diacap.iaportal.navy.mil/ks/Pages/default.aspx

(g) Navy Data Environment (NDE) database (Modernization, Maintenance, Logistics, and Workload & Performance)
https://www.nde.navy.mil

(h) Information Assurance Tracking System (IATS) (Site/System Authority to Operate and DIACAP package status)
https://iats.nmci.navy.mil

(i) Naval Network Warfare Command (NNWC) UNCLAS portal site
https://www.portal.navy.mil/netwarcom/

(j) Defense Information Systems Agency (DISA) Information Assurance Support Environment (IASE) site. http://iase.disa.mil

(k) Vulnerability Remediation Asset Manager (VRAM) site
UNCLAS: https://vram.spawar.navy.mil/# (VRAM 2.0)
UNCLAS: https://iaportal.navy.mil (VRAM 1.0, discontinued)
GENSER: https://www.iaportal.fnmoc.navy.smil.mil (SIPR VRAM 1.0)

(l) NCDOC – Navy Online Compliance Reporting System (OCRS)
https://www.iava.navy.mil/ocrs

(m) SPAWAR SAILOR 2.1 site
UNCLAS: https://sailor.nmci.navy.mil
GENSER: https://sailor.spawar.navy.smil.mil

(n) Defense Information Systems Agency (DISA) Vulnerability Management System (VMS)
UNCLAS: https://vms.disa.mil
GENSER: https://vms.disa.smil.mil

(o) United States Cyber Command (USCYBERCOM) site
UNCLAS: https://www.cybercom.mil
GENSER: https://www.cybercom.smil.mil

(p) Navy Cyber Forces - Cyber Security Inspection and Certification Program (CSICP) Stage 2 Training and Assist Visit portal site.
https://usff.portal.navy.mil/sites/cyberfor/N4/N41/CSICP/
(Compatibility version:
https://usff.portal.navy.mil/sites/cyberfor/N4/N41/CSICP/m/)

(q) U. S. Fleet Cyber Command - Cyber Security Inspection and Certification Program (CSICP) Stage 3 Inspection portal site.
https://www.portal.navy.mil/fcc-c10f/OCA/default.aspx

(r) Total Workforce Management System (TWMS)
https://twms.nmci.navy.mil/

(s) Fleet Training, Management and Planning System (FLTMPS)
https://ntmpsweb.nwptf.nuwc.navy.mil/fltmps/

(t) Joint Personnel Adjudication System (JPAS)
http://www.dss.mil/diss/jpas/jpas.html

(u) U.S. Fleet Cyber Command/C10F Chief Information Officer (CIO) Policy Direction portal
https://www.portal.navy.mil/fcc-c10f/cio/2/PD/default.aspx