Navy Information
Dominance Forces

Commander’s Cybersecurity
Manual

VERSION 4

This manual serves as guidance from Commander, Navy Information Dominance Forces (NAVIDFOR) for Commanders, Commanding Officers (CO), Officers in Charge (OIC), Department Heads (DH), Division Officers (DIVO), and Cybersecurity (CS) Managers regarding the administration of local CS programs and guidance for the Navy’s CS Inspection and Certification Program (CSICP). This document does not cancel or supersede any policy set forth by competent authority and serves to consolidate and amplify existing guidance to enforce sustained compliance and a robust security posture.
# TABLE OF CONTENTS

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANGES</td>
<td></td>
</tr>
<tr>
<td>CHANGE HISTORY</td>
<td>vi</td>
</tr>
<tr>
<td>PREFACE</td>
<td></td>
</tr>
<tr>
<td>INTRODUCTION</td>
<td>viii</td>
</tr>
<tr>
<td>PURPOSE</td>
<td>ix</td>
</tr>
<tr>
<td>SCOPE</td>
<td>ix</td>
</tr>
<tr>
<td>CHAPTER 1</td>
<td></td>
</tr>
<tr>
<td>CS OVERVIEW</td>
<td>1-1</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>1-1</td>
</tr>
<tr>
<td>WHAT IS CS</td>
<td>1-2</td>
</tr>
<tr>
<td>CS AND THE U.S. NAVY</td>
<td>1-3</td>
</tr>
<tr>
<td>DOCTRINE</td>
<td>1-4</td>
</tr>
<tr>
<td>REMARKS</td>
<td>1-5</td>
</tr>
<tr>
<td>CHAPTER 2</td>
<td></td>
</tr>
<tr>
<td>CYBER ORGANIZATION</td>
<td>2-1</td>
</tr>
<tr>
<td>CYBER C2 ORGANIZATION</td>
<td>2-1</td>
</tr>
<tr>
<td>COMMAND-LEVEL CS PROGRAM AND PERSONNEL ASSIGNMENTS</td>
<td>2-5</td>
</tr>
<tr>
<td>CHAPTER 3</td>
<td></td>
</tr>
<tr>
<td>OVERVIEW OF THE CS INSPECTION PROCESS</td>
<td>3-1</td>
</tr>
<tr>
<td>BACKGROUND</td>
<td>3-1</td>
</tr>
<tr>
<td>DISCUSSION</td>
<td>3-1</td>
</tr>
<tr>
<td>CS INSPECTION AND CERTIFICATION PROGRAM (CSICP) STAGES</td>
<td>3-2</td>
</tr>
<tr>
<td>CS INSPECTION (CSI) GRADING</td>
<td>3-3</td>
</tr>
<tr>
<td>AFTER ACTION AND RISK ASSESSMENT</td>
<td>3-7</td>
</tr>
</tbody>
</table>
LIST OF ENCLOSURES:

Enclosure (1)  CS Program Administration Spot Check
Enclosure (2)  Network Security (NETSEC) Spot Check
Enclosure (3)  CS Workforce (CSWF) Spot Check
Enclosure (4)  Traditional Security Spot Check
Enclosure (5)  Afloat/Ashore CS Command Self Assessment
Enclosure (6)  Cyber Zone Inspection
Enclosure (7)  CO’s CS Questionnaire
Enclosure (8)  Minimum Set of Periodic Reports
Enclosure (9)  Semi-Annual Report: Certification and Accreditation (C&A)
Enclosure (10) Monthly Report: CSWF Training
Enclosure (12) Daily/Weekly Report: CS Status
Enclosure (13) Industry Best Practices: SANS Institute
Enclosure (14) Configuration Change Management Process

APPENDIX A  List of References
APPENDIX B  List of Universal Resource Locator (URLS)
APPENDIX C  Glossary of Abbreviations and Acronyms
The following Change History Log contains a record of changes made to this document.

<table>
<thead>
<tr>
<th>Date Published/Revised</th>
<th>Author</th>
<th>Section/Description of Change</th>
</tr>
</thead>
<tbody>
<tr>
<td>28 Oct 11</td>
<td>CDR William Rhea, COMCARSTRKGRU TEN N6</td>
<td>Original Publication</td>
</tr>
<tr>
<td>18 Jan 12</td>
<td>LCDR Hezekiah Natta, NAVCYBERFOR N412</td>
<td>Version 1 of the NCF revision</td>
</tr>
<tr>
<td>26 Feb 13</td>
<td>CDR Cory Brummett, NAVCYBERFOR N412</td>
<td>Version 2. Updated references and URL lists, restructured handbook into 7 chapters, revised or rewrote content, added CS Inspection (CSI) afloat scoring overview, added HBSS overview, revised all existing enclosures, added sample 5050 Notice (Encl 21)</td>
</tr>
<tr>
<td>31 Aug 14</td>
<td>LT Travis Howard, NAVCYBERFOR N75</td>
<td>Version 3. Updated content and terminology, consolidated enclosures 1-5 into 4 Spot Checks, removed obsolete checklists (formerly encl 6-9), removed non-essential IA notices and/or reports, updated references and URL lists, added Industry Best Practices (encl 13) and Glossary of acronyms and abbreviations.</td>
</tr>
</tbody>
</table>
12 Feb 16  | LT Kevin Mott, NAVIDFOR N75  | Version 4. Updated content and terminology, in all chapters and enclosures, removed non-essential IA notices and/or reports, updated references and URL lists, added Weight Summary Average Report to enclosure 11.
          | IT2 Jonathan Salpas,        |          |
          | NAVIDFOR N75               |          |

**Document Properties**

**Owner:** COMNAVIDFOR, Code N7  
**Editor:** Richard Voter (richard.voter@navy.mil)  
**Discrepancies:** Please report any corrections or redlines to NAVIDFOR N7
1. **Introduction.** One only needs to take a look through today’s headlines to understand the security challenges of cyberspace. From information, identity theft, cyber-espionage, criminal hacker activity, to the threat of “insiders” either malicious or unintentional, our Navy networks – afloat and ashore – are at risk. We must stand ready to protect vital information, and secure freedom of movement within cyberspace for our forces. It is with this in mind that the Commander’s CS Manual was developed and refined over the last several years to help Commanders and all levels of command leadership understand the requirements set forth in Department of Defense (DoD) and Navy policies that encompass a command’s CS program. Enclosures (1) through (14) are included to facilitate leadership engagement in this important cyber program. Likewise, the CS Readiness Manual (CSRM), a technical accompaniment to this Manual, was developed to provide further guidance on day-to-day operational practices for a command’s CSWF personnel. The eminent need for these documents stems from several key points:

a. The 2014 Annual Incident/Event Summary Report provided by Navy Cyber Defense Operations Command (NCDOC) noted an increase in confirmed malicious activity across Navy networks, afloat and ashore, by 12 percent compared to 2013. NCDOC noted that defense-in-depth strategies, Information Assurance (IA), CS awareness, and defensive system implementation/refinement afford the Navy the capability to promptly avert and/or mitigate incidents-events and malware infections directed against Navy networks.

b. Inspection results from the CSI process and the Board of Inspection and Survey (INSURV) demonstrate that much command level attention is still required to improve the unit level CS posture and comply with critical CS requirements.

c. Industry best practices, developed and refined by the Systems Administration, Networking, and Security (SANS) Institute and described in enclosure (13) of this Handbook, identify critical security controls proven effective against
Advanced Persistent Threats (APTs) that the Navy can leverage to increase its CS posture across all commands.

2. **Cancellation.** COMNAVIDFORINST 5239.2C

3. **Purpose.** The purpose of this handbook is to provide Navy COs and others in leadership positions an understanding of CS requirements and responsibilities, and how best to leverage their CSWF, techniques, procedures, and available technologies to effectively manage their command CS readiness programs. This is achieved by providing:

   a. An overview of Navy and Joint/DoD command level CS readiness requirements.

   b. References for all command-level CS-related doctrine.

   c. Information on CSWF individual training, education and certification requirements, and resources.

4. **Scope.** This document is intended to provide COs, OICs, DHs, and Division-level leadership with guidelines to best support the command's mission while also protecting and securing Navy physical and virtual networks. Although titled a Commander's CS Manual, the material within is intended to provide a baseline level of understanding for all Navy leaders that are responsible for a command's CS posture. The challenge: Build CS awareness, actions, oversight, and successful execution of CS tasking into the command's daily battle rhythm, and develop technically competent, informed, and proactive supervisors to inculcate cyber readiness down to the deckplates. NAVIDFOR manages this document and solicits your feedback, with lessons and best practices valuable to incorporate into future revisions.

   KELLY AESCHBACH
   Chief of Staff
CHAPTER 1: CS OVERVIEW

1. Background. On 5 January 2012, the President of the United States endorsed new strategic guidance for the DoD that articulated 21st Century defense priorities to sustain U.S. global leadership. Navy Cyber Power 2020, reference (a), is a strategy for achieving the Navy’s vision for cyberspace operations. The Navy must establish and commit to these major strategic initiatives in order to achieve operational success. Cyber Power 2020 serves as a guidepost to inform our enterprise architecture, investment decisions, and future roadmaps.

a. Navy Cyber Power 2020 sets out an ambitious agenda. The strategic initiatives described are critical to ensuring an operational advantage in the maritime domain. Collectively, these efforts represent a fundamental change in the way the Navy conducts operations and network management. Success requires an “all hands” effort, from the Pentagon all the way down to the deck plates.

b. As outlined in the U.S. Fleet Cyber Command/TENTH Fleet Strategic Plan 2015 – 2020: Our vision:

“We will conduct operations in and through cyberspace, the electromagnetic spectrum, and space to ensure Navy and Joint Freedom of action and decision superiority while denying the same to our adversaries. We will win these domains through our collective commitment to excellence and by strengthening our alliances with entities across the U.S. government, DoD, academia, industry, and our foreign partners.”

c. Strategic Goals:

1. **Operate the Network as a Warfighting Platform.**
Defend Navy Networks, Communication, and Space Systems, ensure availability and, when necessary, fight through them to achieve operational objectives.

2. **Conduct Tailored Signals Intelligence (SIGINT)**
Meet the evolving SIGINT needs of Navy commanders through more tailored operations, while continuing to deliver on NSA needs.

3. **Deliver Warfighting Effects through Cyberspace**
Advance our effects-delivery capabilities to support a full
spectrum of operations, including cyber, electromagnetic maneuver, and information operations.

4. Create Shared Cyber Situational Awareness
Create a sharable cyber Common Operating Picture that evolves to full, immediate awareness of our network and everything that happens on it.

5. Establish and Mature navy’s Cyber Mission Forces
Stand up 40 highly experts Cyber Mission teams and plan for the sustainability of these teams over time.

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. In 2015, security breaches into the U.S. Office of Personnel Management (OPM) compromised over 21 million DoD personnel’s personal identifiable information (PII).

f. 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. Cyber Security Defined. Reference (a) defines CS as “prevention of damage to, protection and restoration of computers, electronic communications systems, electronic communications services, wire communications, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.” This definition formally adopts the definition set forth in the National Security Presidential Directive 54, dated 8 January 2008, and the release of the DoDI 8500.01 adopted the term “CS” to be used throughout DoD instead of the term “IA.” CS is about developing operational resilience of our IT infrastructure and managing risk to our networks, ensuring that information and services are available to authorized users whenever and wherever required. Originally developed by the National Security Agency (NSA) and adapted from military strategy dating as far back as the Roman
Empire, the “Defense in Depth” concept for NETSEC is illustrated by Figure 1 (derived from reference (c)):

![Image](image.png)

**Figure 1: The Defense-in-Depth concept (reference (c))**

a. People. Achieving CS readiness begins with senior level management commitment, based on a clear understanding of the threat. This must be followed with effective CS 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 CS services and for detecting intrusions. Given that adversaries can attack a target from multiple points using either insiders or outsiders, an organization needs to utilize protection mechanisms at multiple locations to resist all classes of attack. The Navy’s network architectures are designed to have protection built in at various levels.

c. Operations. This focuses on the activities required to sustain a successful CS program on a daily basis. This includes but is not limited to: C&A, Key Management (Communications Security (COMSEC), Electronic Key Management System (EKMS) program), a CSICP, Afloat Training Group (ATG), and/or Navy Type Commander (TYCOM) assessment.

3. **CS and the U.S. Navy.** CS provides confidentiality, availability, authentication, non-repudiation, and integrity for U.S. Navy IS that enable combat system operations for Assured Command and Control (C2), Battlespace Awareness, and Integrated Fires. IS provides the infrastructure that enables use of the operational platform for information. It is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing,
dissemination, or disposition of information. IS that exist in the U.S. Navy on ships, submarines, aircraft, and expeditionary forces that utilize platform communications systems can be considered a continuously operating forward combat system.

Figure 2: Illustration of a Defense-in-Depth approach to Naval networks, with policies, Standard Operating Procedures (SOPs), and threat awareness providing a strong foundation upon which layered security elements are built and sustained.

4. **Doctrine.** References (a) and (d) define CS requirements for all DoD components.

It is important to note that cyber doctrine and operational plans (OPLANS) are constantly evolving, and impending changes to doctrine follow. Reference (a), initiative 1.2, discusses this evolution in detail:


**Initiative 1.2: Evolve doctrine and OPLANS**

The Navy must fully evolve Navy and Joint operational concepts and OPLANS to take full advantage of cyber capabilities. Cyberspace operations doctrine and tactics, techniques, and procedures (TTPs) are being developed to a comparable level of maturity as traditional warfare areas such as air, surface, and undersea. This enables a broader understanding of how cyberspace operations contribute to the command and control, defense, and operation of all Navy forces and how offensive cyberspace operations are used to achieve operational ends while minimizing the expenditure of ordnance and reducing costs across the range of military operations.

5. Remarks. CS is paramount as the overarching discipline encompassing Information Security (INFOSEC), NETSEC, and Physical Security (PHYSEC). CS incorporates the elements of each type of security into a layered defense that ensures information is readily accessible where and when needed, while ensuring it is protected and defended from adversaries. CS guidance in the Navy is derived from Navy and Joint cyberspace concepts of operations, doctrine, and TTPs. As discussed in reference (a):

**Strategic Initiative 2.2: Change the Culture**

The Navy must overcome cultural barriers impeding the full integration of cyber capabilities through communication, training, incentives, enforcement of policies, and effective governance.

The ability to change the Navy with respect to CS comes through direct leadership and oversight at all levels of the chain of command. Additionally, continuous improvement comes from the evolution of doctrine and operational planning, routine exercises and assessments, strengthening Navy cyber knowledge across the entire spectrum of Navy civilians, officers, and enlisted personnel, and our ability to aggressively pursue leadership of joint cyber modeling, simulation, and analysis (reference (a), p. 6-7).
CHAPTER 2: CYBER ORGANIZATION

1. Cyber C2 Organization. There are multiple commands that make up the Navy’s Cyber C2 organizational construct. Figures 3 and 4 provide an overview of these command relationships, with specific commands outlined in paragraphs below that provide direct support to afloat and ashore units.

---

Figure 3: Navy Cyber C2 Organization
**a. U.S. Cyber Command (USCYBERCOM)** is the sub-unified Cyber Commander under U.S. Strategic Command. 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 communications networks, counter cyberspace threats, and assured access to cyberspace. USCYBERCOM’s efforts support the Armed Services’ ability to confidently conduct high-tempo, effective operations as well as protect C2 systems and the cyberspace infrastructure supporting weapons system platforms from disruptions, intrusions, and attacks. USCYBERCOM sets cyber policy for the entire DoD enterprise.

**b. Defense Information Systems Agency (DISA).** DISA, As a Combat Support Agency, provides, operates, and assures C2, 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 entire DoD Information Network (DoDIN).
c. U.S. Fleet Cyber Command (FLTCYBERCOM)/Commander, Tenth Fleet (C10F). As FLTCYBERCOM, an Echelon II command, it is the Naval component to USCYBERCOM, the sub-unified Cyber Commander. As C10F, an Echelon III command, they provide operational support to Navy commanders worldwide, supporting information, computer, electronic warfare, and space operations. In addition to joint and service reporting, C10F 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 CS compliance on behalf of DISA through the Navy’s CSICP.

d. Program Executive Office for Command, Control, Communications, Computers, and Intelligence (PEO C4I). PEO C4I provides integrated communications and IT systems that enable Information Dominance and the C2 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) and the Consolidated Afloat Network Enterprise System (CANES).

e. Commander, Space and Naval Warfare Systems Command (SPAWAR). SPAWAR 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. NAVIDFOR. As the Navy’s C5I capability TYCOM, NAVIDFOR provides relevant, resilient, and effective C5I capabilities and a highly trained cyber workforce to maximize fleet readiness through Train and Assist Visits (TAVs) to support all Naval missions throughout cyberspace. They are responsible to United States Fleet Forces Command (USFFC) and Commander, Pacific Fleet (CPF) to “man, train, and equip” (MTE) and define requirements for the Fleet on cyber operations in support of FLTCYBERCOM’s CSICP.

g. Naval Network Warfare Command (NAVNETWARCOM). NAVNETWARCOM’s mission is to execute, under C10F Operational Control, tactical-level C2 of Navy networks and to leverage Joint space capabilities for Navy and Joint operations. NAVNETWARCOM operates and defends the Navy’s portion of the DoDIN, current Information Condition (INFOCON) level, and issues tasking orders and guidance to the Fleet in the form of Communications Tasking Orders (CTOs) and Naval Telecommunications Directives (NTDs).

h. NCDOC. NCDOC’s mission is to coordinate, monitor, and oversee the defense of Navy computer networks and systems and to be responsible for accomplishing Computer Network Defense (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 warfighting capabilities for Naval and Joint forces by providing operationally focused training and planning support; developing doctrine, TTPs; 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 Operations Security (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 and post scan analysis), and are commonly partnered with NAVIDFOR’s CSICP Stage II TAVs.

2. CSWF. Reference (e), outlines the CSWF structure. Figure 5 provides a snapshot of various workforce assignments, duties, and functions, however, many of the titles have changed per reference (d) and are noted as such in the following sub paragraphs. Designated Accrediting Authority (DAA), IA Management (IAM), and IA Technical (IAT) functions are replicated within each unit and are described in greater detail below with verbiage directly from references (d) and (e). IA System Architecture and Engineering (IASAE) functions remain with PEO C4I and SPAWAR for PoRs. CNDSP functions reside with NCDOC and C&A functions reside with the FLTCYBERCOM Office of Operational DAA (ODAA).

<table>
<thead>
<tr>
<th>Designated Accrediting Authority (DAA) Functions</th>
<th>Information Assurance Management (IAM) Levels I, II, III</th>
<th>Information Assurance Technical (IAT) Levels I, II, III</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorize connection/testing</td>
<td>Overseer configuration testing</td>
<td>Manage connections/conduct testing</td>
</tr>
<tr>
<td>Accredit System</td>
<td>Oversee System</td>
<td>Administer System</td>
</tr>
<tr>
<td>Authorize IA Controls</td>
<td>Revalidate IA Controls</td>
<td>Manage IA Controls</td>
</tr>
<tr>
<td>Accept Risk</td>
<td>Manage Risk</td>
<td>Operate (in) Risk</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Information Assurance Systems Architects and Engineers (IASAE) Levels I, II, III</th>
<th>Computer Network Defense Service Provider (CND SP) Functions</th>
<th>Certification and Accreditation (C&amp;A) Functions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Develop System</td>
<td>Monitor System</td>
<td>Identify Risk/Audit</td>
</tr>
<tr>
<td>Design IA Controls</td>
<td>Assess IA Controls</td>
<td>Certify</td>
</tr>
<tr>
<td>Engineer (out) Risk</td>
<td>Detect Threat</td>
<td>Recommend Accreditation</td>
</tr>
</tbody>
</table>

Figure 5: CSWF Functional Requirements, reference (g), 1.7

a. CO/Deployed Authorizing Official (AO). The CO is ultimately responsible for the total implementation of the CS program within his or her command, including training and certification of the command’s CSWF. The CO can act as the Deployed AO (previously titled as DAA until redefined by
reference (d)) within the scope and limitations of references (g) and (i). The CO must appoint all Information Systems Security Managers (ISSM), Information Systems Security Officers (ISSOs), and privileged user personnel in writing to manage the command’s CS program, and provide adequate oversight and command involvement in the program.

b. Command Security Manager (CSM). The CSM is responsible to the CO for the proper development, implementation, and enforcement of the command’s personnel and traditional/PHYSEC posture per reference (h). The CSM will work with the ISSM to develop and implement the appropriate traditional/PHYSEC security posture in support of the command’s IS.

c. ISSM. The ISSM is responsible for ensuring the command’s IS is operated, used, maintained, and disposed of per governing security policies and practices. The ISSM should have significant CS experience and is required to be designated in writing by the CO. Navy Enlisted Classification (NEC) 2779 (ISSM) is required of enlisted personnel holding this position who must be appropriately trained and certified per reference (g). Personnel holding the ISSM position at the tactical/shipboard level must be a Chief Petty Officer or above, due to the high level of trust and oversight responsibilities placed upon this position.

d. ISSO. ISSOs are responsible to the ISSM for ensuring the appropriate operational CS posture is maintained for a command. They implement and enforce system-level CS controls per program and policy guidance. In a sense ISSOs are the primary assistants to the ISSM in implementing and enforcing CS policy. ISSOs must be appointed in writing by the CO and be properly trained and certified per reference (g).

e. Privileged Users. Privileged users (e.g., system administrators (SA)) configure and operate the network within the authorities vested in them according to CS policies and procedures. Privileged users are typically of the Information Systems Technician (IT) or Cryptologic Technician (CT) ratings, but may be another rating provided they are properly trained and certified per reference (g). Privileged user personnel administer and maintain a command’s IS, and are the backbone of the CSWF.
f. Authorized Users. Authorized users of a network system must report CS-related events (e.g., negligent discharges also known as data spillages) and potential threats and vulnerabilities (e.g., insider threats) to the appropriate ISSO or the ISSM. Users must also protect information commensurate with the classification or sensitivity of the information accessed, protect network equipment within their spaces from unauthorized access, observe local policies and procedures governing the secure operation and authorized use of the command’s network resources, and meet minimum CS awareness training requirements as a condition of access. They must also participate in annual Cyber Awareness Challenge training as mandated by the DoD.
CHAPTER 3: OVERVIEW OF THE CS INSPECTION PROCESS

1. Background. CSICP is the Navy’s process of formally inspecting the CS programs and current readiness posture of afloat and ashore commands per DoD, DON, DISA, and National Institute of Standards and Technology (NIST) standards. The CSI is conducted part of the Navy’s CSICP by FLTCYBERCOM’s Office of Compliance and Assessment (OCA) for all Navy commands, and utilizes the same inspection format and standards as DISA’s Command Cyber Readiness Inspection (CCRI). The grading criteria, as of 16 January 2015, is currently in “Phase IV” implementation as directed by DISA. FLTCYBERCOM OCA will consider a ship’s Optimized Fleet Response Plan (O-FRP) cycle whenever scheduling a CSI, coordinating with a command’s Operational Fleet Commander or Echelon III as part of the Fleet scheduling process. The three stages of the Navy’s CSICP have been validated by Commander, Naval Air Forces, Commander, Naval Surface Forces, and Commander, Naval Submarine Forces as part of their respective Inspection, Certification, Assessment, Visit (ICAV) event list. First notification of a command’s CSI normally occurs 6-9 months prior to the inspection date, allowing for time to complete Stage I and II reviews. If a command established and is maintaining a robust CS readiness program, preparation for the CSI should cause minimal impact.

2. Discussion. Notification of the CSI schedule occurs via release of a FLTCYBERCOM OCA CSI Schedule message. Any changes to this schedule will be promulgated by message update. FLTCYBERCOM OCA will formally contact a command approximately 120 days prior to their inspection to begin formal coordination. NAVIDFOR CSICP Stage II TAV Teams, partnered with NIOC NBT personnel, are a resource available to commands to train, assist, and help self-assess a command’s CS readiness. In doing so, the CSICP Stage II TAV provides a command a CS discrepancy list with recommended improvement actions to help the command prepare for a CSI and to maintain the highest level of CS readiness. Stage II teams provide command personnel training on best practices and current tactical directives. NBT personnel will perform a network operational behavior assessment, to include a post assessment T-rating report, covering all operational behavior areas that are included in the Operational Behavior portion of a Navy CSI. Outside assistance aside, a command’s very best preparation for a CSI is to maintain daily
vigilance and attention to detail in all areas of CS readiness, to include periodic spot checks and status reports to command leadership. Enclosures (1) through (5) are designed to assist command leadership and CSWF personnel preparing for a CSI. Enclosure (7) provides Commanders and OICs with a range of questions to initiate a self-assessment of CS 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 two-day review, scheduled and conducted by a command’s Immediate Superior in Command (ISIC). This review consists of an internal review of CS administration, leadership engagement to include CO’s policy, CSWF personnel training and qualifications. Units preparing to receive a Stage I ISIC Review should use this handbook, as well as NAVIFOR 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 (p). A thorough review and implementation of day-to-day practices outlined in reference (a) is also recommended to build a sustainable CS posture. Enclosure (3) of the NAVIFOR CS Manual (CSRM) provides a preparation guide and timeline that should be considered as early in the process as possible. Upon completion of a Stage I or 90-days prior to a Stage III, a command should coordinate their Stage II unit level TAV.

   b. Stage II: Unit Level TAV. This is a nominal five day evolution scheduled and executed by Echelon II commands. For afloat units, as well as USFFC, CPF, and FLTCYBERCOM subordinate commands, Stage II TAVs are conducted by NAVIFOR. **Note:** NAVIFOR is not resourced to conduct Stage II TAVs for all Navy commands but will support as requested and as schedule, availability, and resources allow. The Stage II TAV includes a review of Stage I, plus an additional in-depth assessment of network security, PHYSEC, administration, training, personnel, operations, and monitoring. Upon 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 FLTCYBERCOM OCA.
(1) For NAVIDFOR-conducted Stage II TAVs, the assessment will contain an accompanying NIOC NBT element who will perform network scans to be analyzed post-TAV as a NBT Network Operational Readiness Assessment, or NBT Assessment (NBTA). The NBTA report is provided to the command and their ISIC via Secure Internet Protocol Router Network (SIPRNet) e-mail within 2-3 weeks of the TAV. The NBTA provides an overall T-rating, broken-out into 4 T-rated subareas. In most cases the NBTA will be forwarded to the unit via NAVIDFOR N7, CSICP Stage II TAV sponsor.

(2) It is important to distinguish the NBT’s T-score, which measures operational behavior risks to the DoDIN, from an overall CSICP Stage III CSI score. NAVIDFOR Stage II TAVs do not perform CSI pre-inspections or provide a post-event score. Instead, a command will receive a comprehensive Stage II TAV out-brief along with an extensive list of findings that will assist a command in preparing a Plan of Action and Milestones (POA&M) to address any CS program deficiencies and to build a more robust command CS program, which should help the command prepare for a CSI and to maintain the highest state of cyber readiness.

c. Stage III: CSI. This is a nominal 5-day comprehensive graded inspection conducted by FLTCYBERCOM OCA encompassing all DISA CCRI CS areas, specifically: leadership engagement, physical (traditional) security, administration, training, network configuration, and network operations. Stage III CSIs will result in a single grade for each classification of network inspected (unclassified-but-sensitive, and classified, as applicable) that represents an evaluation of CS requirement compliance measured against unmitigated CS vulnerabilities to the DoDIN.

4. CSI/CCRI Grading. FLTCYBERCOM uses the CCRI grading criteria controlled by USCYBERCOM and managed by DISA’s DoDIN Readiness & Security Inspection (DRSI) office. What distinguishes a Navy CSI from a USCYBERCOM CCRI is the report of findings requirement; CCRI results are reported to USCYBERCOM while CSI results are reported to FLTCYBERCOM. Additionally the CSI has an inclusion of an assessment of the command’s operational behavior by the NBT. Navy commands can expect to be graded against the four primary inspection pillars illustrated in Figure 6:
a. Program Administration (10 percent of overall grade). Also known as “Contributing Factors” and divided into three focus sections: culture, capability, and conduct. This area inspects command policies, reviews documentation of required command programs and procedures, standardized reporting, contingency plans, and training plans. All of these areas are all within a CO’s control.

b. Network Configuration (60 percent of overall grade). Comprising the largest part of a command’s overall grade, this area gathers vulnerability data across a wide variety of technology focus areas. Vulnerability Management of network connected PoR systems, internal network enclaves, traditional security, and cross domain solution compliance (as applicable) is included in this portion of the inspection. Some fixes in these areas are PoR dependent and beyond a CO’s ability to control remediation. The CO should know the status and have communicated outstanding issues with their TYCOM and NAVIDFOR.

c. CND Directives (30 percent of overall grade). This area grades compliance of Operational Orders (OPORDs), Fragmentary
Orders (FRAGOs), Tasking Orders (TASKORDs), and Computer Tasking Orders (CTOs). The graded orders are selected by USCYBERCOM and DISA as part of the standard joint service CCRI grading criteria.

d. Operations Behavior (up to 25 points subtracted from overall score, depending on findings). A grading tool unique to Navy CSIs, Operations Behavior is assessed by NIOC NBT automated network scans and observations made by the inspection team. Scans search for unauthorized user behavior such as Universal Serial Bus (USB) violations, unapproved web browsing behavior, evidence of malware or unauthorized user network intrusion, unauthorized open ports and protocols, and outdated anti-virus scanning programs. Findings are weighted based on category, with an overall risk value then subtracted from the command’s CCRI score to arrive at the final Navy CSI score. Mitigation of this area is within the command’s control.

5. Afloat CSI Grading. As described in the previous section, FLTCYBERCOM applies DISA established, USCYBERCOM approved, and joint service standard grading criteria when conducting CSICP Stage III CSIs. This overall grade, which encompasses PoR findings, does not effectively convey to afloat commands the level of aptitude and CSI performance of the crew. While understood that unmitigated PoR vulnerabilities are important when assessing a command’s network overall risk to the DoDIN, starting in June 2012, FLTCYBERCOM developed a separate score for afloat units that grades ships based on that portion of the overall CCRI that is determined controllable “inside the lifelines.” This demonstrates leadership engagement and involvement in their CS posture and does not penalize them for non-compliant PoR systems beyond their control. Figure 7 illustrates how a Stage III CSI score may be displayed during a CSI out-brief, differentiating the Ship’s Force score (excluding PoR findings) from the overall score (including PoR findings).
Figure 7: Afloat Scoring Format

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 Ship’s Force 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 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 reference (j), 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 CSI scoring across the four inspection areas:

(1) Program Administration (10 percent)

(2) Network Configuration (60 percent)
(3) CND Directives (30 percent)

(4) Operational Behavior (up to -25 percent)

c. To more accurately reflect readiness, the following grading categories will be used for the Ship’s Force adjusted score:

(1) 90 percent or better: Outstanding. Strong CS environment with minimal risk to the DoDIN.

(2) 70-89 percent: Satisfactory. CS environment within acceptable risk to the DoDIN.

(3) Below 70 percent: Unsatisfactory. CS Environment is a potential risk to the DoDIN.

6. After Action and Risk Assessment. No later than five working days following a Stage III CSI, commands must submit an after action report with their POA&M to remediate any found critical areas of concern. Additionally, commands must submit a risk assessment within that same time period. The purpose of the risk assessment is to identify and prioritize actions required to mitigate those items presenting the highest risk to the command’s mission and to the DoDIN. To facilitate the risk assessment, commands are provided with the following by FLTCYBERCOM OCA at the conclusion of the Stage III CSI: (1) inspection out-brief, (2) risk indicator scores for all inspected network enclaves, (3) threat analysis from NCDOC, and (4) a risk assessment “way ahead” template.

a. In addition to the inspection score and outbrief, inspection findings will be further assessed by the inspection team to provide a quick-look risk indicator. The risk indicator gives a low/medium/high descriptor for 16 different line items as well as an overall low/medium/high for each inspected network enclave.

b. In the event the command fails the FLTCYBERCOM OCA CSI a Quarantine Review Board (QRB) is conducted. FLTCYBERCOM OCA has the authority to disconnect Navy systems that pose a significant risk to the Navy DoDIN. They will ordinarily coordinate with the affected echelon II commander to conduct the QRB on those actions that could limit the operational capabilities of the affected commander prior to ordering such actions. The QRB is a technical review, in close coordination with the echelon II
operational owner, to assess identified systems with high threat vulnerabilities that pose a level of risk to the DoDIN that warrants disconnection. The QRB recommendation is provided to FLTCYBERCOM for decision.

c. A threat analysis, provided by NCDOC, covers a period of 360 days and provides information on historical incidents, APTs, previously seen attacks, and any mission impacts regarding previous attacks. This information is provided to each site to improve CS situational awareness and the command’s understanding of how the adversary is specifically targeting that command. It will also promote greater understanding of how internal incidents could have a larger impact on CS. This reports the risk assessment and enables the command to focus defensive measures and assess the effectiveness of their CS program.
CHAPTER 4: PROGRAM ADMINISTRATION AND TRAINING

1. Discussion. Development of a command CS program begins with the CO ensuring the establishment of local directives and enforcing training requirements. This is the cornerstone to a successful command cybersecurity program; the CSI grading criteria refers to these measures as “contributing factors” (see Chapter 3, paragraph 4a.). While DoD, Secretary of the Navy (SECNAV), and Chief of Naval Operations (CNO) instructions set policy on an enterprise level, they are not designed to provide guidance at the tactical level to your specific network configuration. Thus, COs must ensure local policies are created based on this existing guidance to provide their network users with a framework for network behavior per best CS practices.

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

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

   b. Reference (g) 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 NAVIDFOR, N1 Directorate, as the executive agent for CSWF management within the Navy.

   c. Reference (l) is the DoD governing instruction on Incident Response, and reference (m) provides specific Navy policy for developing an Incident Response program locally. Reference (n) is the NTD that addresses Electronic Spillage (ES)/Negligent Discharge within the Navy enterprise, and must be incorporated into a local command Incident Response Plan.

3. Requirements. The following requirements are derived from the above references and CCRI/CSI grading criteria:
a. Command leadership engagement. Enclosure (8) outlines a minimum set of periodic reports from the command ISSM to the Commander or CO and will be tailored at the local level. Additionally, commands will implement enclosures (1) through (5) as command leadership spot checks. Enclosure (6) is provided for commands to incorporate into their local zone/space inspection program. These reports and processes allow command leadership to stay engaged and informed. Finally, the CSRM, available via URL (o), provides recommended guidance for technical personnel and can be used as a reference for commanders to implement a CS battle rhythm.

b. Authorization to Operate (ATO). All commands must maintain an ATO for their network systems, described in reference (o) as granted by the AO for an IS to process, store, or transmit information. An ATO is granted after the AO reviews the security authorization package, determines risk to organizational operations, and makes a risk control decision expressed as an ATO, interim authority to test, or denial of ATO (DATO). Once an ATO is granted, the Authorization Termination Date (ATD) is typically within three years of the authorization date. Under PoR direction, afloat commands fall under a “Type Authorization” and are responsible for a single authorization package (known as the “site ATO”), while PoR are responsible for the cognizant system’s authorization process. Command ISSMs are trained in the Certification and Accreditation (C&A) process and must ensure all C&A documentation is retained and tracked. Six months (180 days) prior to a site’s ATO expiration, the ISSM must contact their ISIC and begin to review and update the security authorization package for approval by FLTCYBERCOM ODAA. Reference (au) includes guidance from FLTCYBERCOM ODAA regarding C&A testing and validation procedures under the DoD IA Certification and Accreditation Process (DIACAP) program (see below note).

NOTE: Reference (a), issued 14 March 2014, effectively terminated DIACAP as the DoD’s IT accreditation process in favor of a “multi-tiered CS risk management process” as described in NIST Special Publication (SP) 800-39 and directed per reference (o), which was updated and reissued on 12 March 2014 as the “risk management framework (RMF) for DoD IT.” As this process matures and is integrated into the Navy’s acquisition and ATO renewal process, further guidance will be promulgated by FLTCYBERCOM ODAA.
c. Command CS Policy. Reference (d) provides specific policy requirements that must be translated into local policy, typically via a local command instruction and/or Standard Operating Procedures as directed by reference (e). Specific instructions that should be included in every local CS policy are outlined as follows:

(1) Configuration Management (CM). Per reference (k), afloat and shore sites are required to place all DoD IS under the control of a locally chartered Configuration Control Board (CCB). Membership in the CCB should include SA and CS personnel, and be designated in writing in a collateral duties notice or instruction. The CCB should meet regularly, at a minimum quarterly, and be incorporated into the ISSM’s weekly schedule. Commands will retain historical documentation of CCB meetings and logs of configuration changes to the network, as this documentation will be inspected as part of a CSI. For afloat units, this entails maintaining a combat systems “smooth log” that tracks configuration changes to the network and is reviewed by the ISSM regularly, with monthly or quarterly meetings to go over changes in procedures and keep the chain of command informed. To ensure proper CM, units should follow the workflow outlined in enclosure (14).

(2) Vulnerability Management (VM). Per reference (k), “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 issued Information Assurance Vulnerability Management (IAVM) patches or Fleet Advisory Messages (FAM)) that endanger the confidentiality, availability, authentication, integrity, and non-repudiation of the information and IS. Commands are responsible for ensuring system compliance for newly-acquired assets are verified before being placed on the operational network or a System Operational Verification Test (SOVT) is signed. Command personnel must maintain communications with the program office for a given system, and refer to them for vulnerability patching and baseline updates. They must also ensure system baselines are maintained (e.g., for ISNS), comply with SPAWAR baseline instructions in the ship’s Software Version Description Document (SVDD) found via URL (l), SOVT and retain any PoR or vendor-provided system documentation (e.g., software upgrade kits). This also applies to all re-imaged machines in which
all current software upgrades and patches must be re-applied prior to connection with the network. The CSRM, available via URL (o), includes SOPs for conducting vulnerability management through patching and scanning systems. Patch delivery software (i.e., Windows Server Update Services (WSUS)) depends on the PoR. Scanning software currently in use for afloat and ashore commands is the Nessus Scanner, which is a component of the Assured Compliance Assessment Solution (ACAS). The eEye Retina tool, part of the Secure Configuration Compliance Validation Initiative (SCCVI) has been replaced by ACAS and is no longer applicable. Afloat platforms have received ACAS implementation guidance via FAM from PMW 130, per reference (s).

d. Command Incident Response and Recovery (CIR&R). Networks are never 100 percent secure, and it is crucial that commands develop a repeatable process for reporting intrusions, incidents, and network information or electronic spillages/negligent discharge quickly and effectively. The Navy’s Tier 2 CNDSP, NCDOC, is responsible for providing guidance for IR&R. Additionally, reference (k) provides instructions for incident response planning. Also, URL (e) should be used and referenced in the instruction for the most up-to-date direction from NCDOC. Per reference (t), command personnel who are responsible for executing the IR&R plan must be trained and the plan must be exercised and updated at least annually (for networks that are Mission Assurance Category (MAC) level II or III) or semi-annually (for networks that are MAC level I). For example, many integrated afloat networks fall under MAC level II criteria; refer to the system ATO for the specific MAC level and inherited controls that they are applicable to. After action reports, lessons learned, and all other incident-related training or documentation must be retained showing the plan is exercised, reviewed, and updated as appropriate.

e. Continuity of Operations Plan (COOP). Development of a local COOP is critical for shore commands to have the ability to sustain mission essential functions in the event of a man made 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 measures are covered in the Planned Maintenance System (PMS) or established SOPs.
f. CSWF Improvement Program (CSWIP). References (e) and (u) must be read and understood by all command ISSMs, as these serve as the backbone for training and certifying the CSWF. Individual commands administratively manage their CSWF program via URL (q), the Total Workforce Management System (TWMS). This online database consolidates and reports certification and training requirements for all workforce members and must be regularly viewed and tracked by command leadership. It must be properly maintained at the local level to provide Fleet commanders an accurate CS readiness assessment. Commands must develop a local CSWIP per reference (g). The ISSM, as the CSWF Manager, must maintain and provide training plans for all workforce members, and ensure all SAs are both properly trained and designated in writing with signed Privilege Access Agreements (PAAs). Navy “A”, “C”, and “F” school requirements are outlined for units via URL (r), available to the command’s Training Officer, and should be referred to often as CS and IS schools are updated.

4. Training Opportunities. Afloat units must follow Fleet Training Management and Planning System (FLTMPS) requirements, including applicable “C” and “F” school requirements. NAVEDTRA 43469 (series), Personnel Qualification Standard (PQS) for Information Assurance, or the Job Qualification Requirement (JQR) equivalent for civilian personnel, is required by all CSWF members at all levels and directs the appropriate training necessary prior to qualifying as a technician or manager. PQS/JQR training can be accomplished by a command-qualified Subject Matter Expert (SME) and on-the-job training (OJT). Additional training, or emphasis on a particular Course of Instruction (COI), is provided as follows:

a. Computer Network Team Trainer (CNTT). The CNTT course is available at NIOC Norfolk and NIOC San Diego. Students learn to apply the TTPs needed to defend shipboard networks against intrusions and exploitations. Tools are demonstrated in a structured "brief and use" setting where students are able to apply mitigation techniques to attack in an environment that mimics a shipboard network. The course also provides an overview of the NBT mission and capabilities.

   (1) Scope. This five day course provides an overview with detailed discussion of network defense for shipboard networks. Discussions include general and specific threat briefs, access control list management, intrusion detection system management, password assessments, system scanning, and use of third party utilities in the conduct of defensive cyber
operations. Additional information is drawn from systemic fleet wide cybersecurity issues identified during navy blue team assessments.

(2) Target Audience. Although useful for shore-based Information System Technician (IT) personnel, this course is designed for shipboard IT and other personnel tasked with Defensive Cyber Operations (DCO) and computer network defense on U.S. naval vessels. There are no prerequisites; however, the training is most effective if the attendees have a basic understanding of network system administration in active directory and operating system fundamentals.

(3) Schedule. CNTT is most effective when attended during the unit(s) basic phase of O-FRP and prior to a Navy Blue Team assessment. NIOC Norfolk/NIOC San Diego will coordinate with appropriate type commander and unit for specific dates. Contact the following points of contact for further information and course scheduling: Mr. Joe Streer (NIOC Norfolk), 757-417-7100, joseph.v.streer1@navy.mil; Mr. Jay Rutter (NIOC San Diego), 619-545-4588, jay.rutter@navy.mil.

b. HBSS. All personnel with privileged access to the command’s HBSS suite must be properly trained prior to operating the system. HBSS SA should attend the HBSS “Basic” Version 4.6.8 course, Course Identification Number (CIN) W-150-2130 (1 week). Graduates of the Basic course must attend follow-on advanced training, (CIN) W-150-2160 (1 week). Completion of both COIs will provide HBSS SAs 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 SA to operate, possessing Security Plus (+) certification and journeyman-level network administration experience (NEC 2791 is a prerequisite to attend training). Note that current Basic/Advanced courses are being used as required “F” schools until curriculum can be incorporated into NEC 2780, Network Security Vulnerability Technician (NSVT), expected in FY16. Additional HBSS training, including online/virtual training, is available via the DISA IA Training Portal, URL (b). ISSMs must also attend training, or complete the DISA online equivalent, prior to obtaining “global reviewer” access to HBSS.

c. Leadership Seminars and Training. Leadership-level courses, such as the ISSM course (CIN A-531-0009), provide valuable information pertaining to CS. It is also highly
encouraged for ships to “deepen their bench” whenever possible by sending multiple CS leaders (including junior officers) to this course when the operational schedule allows. Without this valuable classroom instruction, division and command leaders miss critical baseline professional training that can assist a command in better implementing their CS program. Additionally, NAVIDFOR N71 conducts periodic waterfront CS seminars and conferences, targeting CO/Executive Officer (XO)/DH and ISSM levels, which are designed to raise awareness and answer questions regarding individual command CS requirements, successful practices, and the overall CSICP process. Further information can be found via NAVIDFOR, Fleet Commander, and Regional TYCOM periodic announcements in message traffic, ISIC correspondence, and via NAVIDFOR’s CSICP Stage II TAV website, URL (o).

5. CS Program Binder. Commands will develop and maintain a “program binder” that consolidates DIACAP documents, local CS instruction, 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 CS program.

6. Monitoring and Assessment. Reference (c) directs that all DON CS programs must be periodically evaluated for effectiveness. Evaluation must take place at all levels, from the duty SA to the applicable DON oversight agency to ensure DON IS continues to adapt to an ever-changing threat environment. The axioms “you get what you inspect, not what you expect,” and “trust but verify” are particularly true in the realm of CS. The CO should apply the same level of attention and scrutiny to CS as they do to EKMS management. Commands with the most robust CS assessment and monitoring programs are best equipped to operate and defend in the cyber domain.

   a. CS Quick Look. Enclosure (7) provides a CO’s CS Program Questionnaire as an example of questions COs should ask their designated ISSM in order to obtain a status of their command’s cyber readiness. The quick look touches on all areas of CS and can be used by management to determine if more extensive processes for maintaining the command’s cyber readiness posture are necessary.

   b. Periodic Reports. Enclosure (8) lists a minimum set of reports for COs to review periodically to get a sense of the overall CS health of their command.
c. Spot Checks. Command CS programs encompass a wide array of auditable data. The check sheets in enclosures (1) through (4) provide specific items to check in several key areas.

d. Zone Inspections. The command zone inspection program is a great place to engage the command’s INFOSEC team. Enclosure (6) provides suggested CS items to be reviewed during zone inspections.

e. Self-Assessments. The checklist contained in enclosure (5) will assist commands in conducting periodic self-assessments, and URLs (o) and (p) offer checklists from the CSICP process that can be used as an additional method for command self-assessment. The ISIC N6 should provide even further insight and “outside looks” to ensure the command programs are in compliance with the most recent CS policies and procedures. Commands must conduct self-assessments semi-annually, concurrent with security self-assessments by the CSM.

7. Training and Assistance. For additional guidance, templates, and tools, refer to URLs (o) and (p). Commands are encouraged to maintain regular communication with their ISIC, TYCOM, and ID TYCOM to stay current on the latest CS policy changes, best practices, lessons learned, and train to the latest version of the CSRM, which is updated quarterly and posted to URL (o). Evaluate and incorporate these lessons learned and best practices into recurring processes, daily network operations, and IS maintenance practices.
CHAPTER 5: NETWORK TECHNOLOGY

1. Discussion. Network technology as it pertains to CS 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 CS. In addition, an overview of the HBSS is provided.

2. References. The following references pertain to using network technology to perform CS:

   a. References (u) and (v) are tactical directives to DoD and naval forces requiring technical implementation at the site level, and are reviewed by command personnel to determine applicability and compliance reporting.

   b. Reference (w) contains requirements for commands with approved cross domain solutions (automated process for moving data from a higher classification system to a lower classification system and vice versa).

   c. Reference (x) contains DoD-level direction from USCYBERCOM and DISA on the deployment and operations of HBSS, with reference (y) providing implementation guidance specific to naval components.

3. HBSS. DISA, in support of National Security goals established by the President, purchased a capability that develops and deploys an automated host-based security solution for network administrators and security personnel. This system provides mechanisms to prevent, detect, track, report, and remediate malicious computer-related activities and incidents across all DoD networks and IS. Figure 8 illustrates the HBSS concept:
Figure 8: HBSS architecture overview, showing a typical afloat installation (left), and data roll-up scheme to the Service or Agency-designated CND Service Provider and DoD Enterprise (right).

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

b. The governing directives pertaining to HBSS are outlined in reference (x), with corresponding Navy guidance outlined in reference (y). Specifics on the guidance contained in these references include:

(1) Installation of various software security modules required on all compatible DoDIN-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 the Virus Scan Enterprise.

(2) 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 HBSS Secure Site status is achieved, the firewall component of HIPS will be activated to provide additional NETSEC and authorized network device connectivity. Note that for units under SPAWAR PMW-130 configuration management requirements for the CND-OSE PoR, CTO 13-17 directs secure site mode for all classified networks. NIPRNet will be promulgated via separate CTO at the direction of the PoR in coordination with NCDOC.

(3) Administrators must ensure all subnets within each enclave are actively monitored in HBSS by the Rogue System Detection (RSD) module. Knowledge of the site’s specific network topology is required to deploy rogue sensors 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).

(4) The ISSM 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 series for each version of HBSS fielded to the Fleet, and discussed in greater detail in the CSRM, available via URL (o). A dashboard entitled “Site Compliance” (installed with the system) will provide administrators with knowledge of assets that are not compliant with reference (x).
(5) It is imperative that the ISSM 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 ISSM to view events, alerts, and logs in HBSS without requiring privileged access.

4. Requirements. Using the references outlined in paragraph 2 above, commands are to be compliant with the following network technology requirements as they pertain to CS:

   a. Password Management. For all systems, the ISSM 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 Standard Form (SF)-700 and stored in a General Services Administration (GSA)-approved container appropriate for the classification level of the system.

   b. IAVM. The IAVM process is designed to provide positive control of the vulnerability notification and corrective action process in the DoD. Commanders will comply with the IAVM process and report compliance to the appropriate combatant commander and to NCDOC via the Vulnerability Remediation Asset Monitor (VRAM), URL (k). Compliance is then verified by Retina or ACAS. Commands must monitor that patches deployed were implemented and reported. Any patches not installed properly will be reported to the applicable system Program Management office via global distance support service ticket (Navy 311). 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 analyze the vulnerability, and if they find the vulnerability has the potential to impact DoD operations, they issue a vulnerability notice in the form of an Information Assurance Vulnerability Alert (IAVA), an IAV Bulletin (IAVB), or IAV Technical (IAVT) notice, depending on severity.
(3) NCDOC, as the Navy’s CNDSP, coordinates a technical review of the vulnerability with SPAWAR to determine applicability to Naval networks. NCDOC will then issue a tailored IAVA, IAVB, or IAVT message to the Navy.

(4) The PoR 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 VRAM site, URL (k), that a patch is available for applicable affected systems.

(5) NAVIFOR is working to get all PoRs to post patches to SAILOR 2.1 but currently patches may be found in alternate locations as well. Navy commands receive an announcement via FAM or other notification, most commonly a Mandatory Security Update (MSU) from the PM, that a series of vulnerability patches have been tested and are now available with instructions on how to obtain the patches.

(6) Navy commands apply the patch to the system. For non-PoRs, the command downloads the patch directly from the DoD patch repository, while PoR controlled system patches will be released by the cognizant program office. For non-PoR networks controlled by a contracted vendor (e.g., a Total Ship Computing Environment such as those installed on the most modern platforms), follow direction provided by the contractor for all patch implementation.

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

c. ACAS. Reference (p) remains germane, amplified for commands in both references (q) and (r), and must be read and understood by command ISSMs. All commands must maintain up-to-date scanning software as instructed in reference (z), located via URL (l). Scans must be conducted on a monthly basis for all network-connected PoR systems (not just “ISNS COMPOSE” for afloat units) to include GCCS-M, ADSI, NTCSS, Navy Cash and CND-Operating System Environment (CND-OSE, the HBSS server suite) and others. Regardless of the software patching technology in use (e.g., IAV Manager for COMPOSE, or WSUS) administrators must adopt a “scan-patch-scan” methodology as described in these references and the CSRM to ensure patches are properly applied across the network. For all commands with PoR networks (e.g., ISNS COMPOSE), the VRAM site is used to store and analyze RETINA or ACAS scans, accessed via URL (k). For all others, the
approved repository is the DISA-managed Vulnerability Management System (VMS), accessed via URL (m). Commands must ensure an archive of the past 90 days’ worth of scans exist in VRAM/VMS or are held locally.

d. Anti-Virus (A/V) Updates. A/V definitions must be kept updated to ensure proper network security. 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 maintained within a seven-day periodicity by requirement, and if configured correctly, automated update servers will check for updates daily. With VRAM 2.0, URL (k), A/V reports are now available as part of the scanning process.

e. HBSS. Observed compliance with reference (x) continues to challenge the Fleet as the level of training and technical implementation varies from site-to-site. Commands must review this reference, as well as future correspondence to Naval components in the form of NAVNETWARCOM (CTF 1010)-issued CTOs or PoR-based FAMs, to ensure local ISSMs are current on the latest implementation guidance. HBSS is a crucial component of a command’s CS posture and understanding the capabilities of this system is vital. HBSS Basic and Advanced training classes and DISA Online Training are available in chapter 4.

f. Compliance with USCC OPORDs, TASKORDs, CTOs and SPAWAR FAMs. Reference (v), 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 ISSMs must track and report CTO compliance to command leadership, ensuring the proper reports are made “outside the lifelines” as well, and use 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 SA. 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 (aa) and reference (ab) provides specific instructions to commands regarding the implementation and enforcement of PKI requirements. Per 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 (Note ISNS COMPOSE Version 3.5 or
higher with RAPIDS installed are UBE capable and must comply with UBE standards). Reference (ab) 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 percent enforcement, as this has the potential to cause problems in a bandwidth constrained environment. Complete details can be found in references (aa) and (ab). Consult PoR guidance for implementation instructions.

h. STIGs. 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. SAs should verify compliance with all STIGs that apply to their IS components on a semi-annual basis; for PoR systems, PMs promulgate guidance for STIG compliance. **Commands should not attempt to comply with STIG direction on their own without PM instruction.** 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 for appropriate action.

**NOTICE TO AFLOAT COMMANDS:** Due to network configuration management controls, do not attempt to implement STIGs without first consulting the applicable PM (e.g., SPAWAR) for guidance. Failure to do so can result in degraded system(s) performance and/or loss of system access or 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. Consult PoRs and command-designated CCB members for guidance on the use of those tools.

(2) Failure to consult PoRs on configuration changes to ensure continued system functionality before implementing a STIG configuration change may disable/degrade the networks and IS.

g. USB Scans. Reference (ac) suspended the use of removable flash media on Navy networks. Available for download via URL (o), the NSA developed USB device detection tools that scan network hosts (client workstations) for unauthorized USB activity. When questionable USB activity is discovered, SAs
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 CS policy, command SOPs and account user forms will clearly state permitted and prohibited USB use and provide appropriate enforcement authority to CSWF personnel. As with RETINA and ACAS scans, common problems 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 (o) and (p). Commands are encouraged to maintain regular communication with their ISIC and TYCOM to stay current on the latest policy changes, best practices, and lessons learned. These lessons learned are codified in the CSRM. Evaluate and incorporate these lessons learned and best practices into CS, daily network operations, and maintenance practices.
CHAPTER 6: TRADITIONAL SECURITY

1. Discussion. The Navy’s Information Security (INFOSEC) Program involves the classification, safeguarding, transmission, and destruction of classified information. The DoD Traditional Security Program encompasses physical, personnel, industrial (Contractors), and information. Traditional Security, as it relates to a command’s security program, is derived from DoD (DISA) requirements and STIGs. The Command Security Manager (CSM) is responsible for these STIGs and should be coordinating closely with the Command ISSM to ensure compliance. A proper Traditional Security program is evident throughout the command and starts with visitor/access control at the entry control point/QD all the way down to physical access to network drops in classified spaces. Traditional SMEs are responsible for training the CSM and ISSO and/or ISSM on DoD requirements and STIGs as they pertain to the Cyber Security. The CSM is responsible for all STIGs listed on the Traditional Security Checklist, to include those referencing Automated Information Systems (AIS). In these instances, the CSM and ISSM will coordinate efforts and ensure that DoD regulations are being followed and properly documented via command instruction, SOP, or both. The Command Security Program not only requires a properly trained security officer and security staff, but continuous security training of all personnel onboard.

2. References. The following references pertain to Traditional Security. SECNAV Instructions can be used in conjunction with DoD Instructions, if more stringent. Command CSMs will be knowledgeable of these references:

   a) DoD 5200.01 Volume 1 (General)
   b) DoD 5200.01 Volume 2 (Marking)
   c) DoD 5200.01 Volume 3 (physical)
   d) DoD 5200.01 Volume 4 (CUI/PII)
   e) SECNAVINST 5510.36
   f) SECNAVINST 5510.30
   g) DoD 8100.02 (Wireless)
   h) IA PUB 5239-22 (Closed Storage)
   i) DoD 5230.20 (Foreign National)
   j) Joint Personnel Adjudication System (New Account Instructions)
   k) IASE Website (CAC Enabled)
   l) NAVIDFOR CSICP Training Website
3. **Requirements.** The following requirements are derived from the above references and lessons learned from the CSICP inspection process regarding command enforceable/non-Program of Record Traditional Security requirements:

   a. **Foreign Nationals (FN).** Foreign National Notification. Commands that have foreign nationals (Personnel Exchange Program (PEP)/Foreign Liaison Office (FLO)) must have a Delegation of Disclosure Authority Letter (DDL) or equivalent written disclosure for each FN, detailing classified access. Commands that have foreign national visitors, and/or Personnel Exchange Program (PEP)/Foreign Liaison Office (FLO) personnel assigned to their commands must ensure a standard operating procedure or command instruction is in place that instructs the crew of the access limitations of foreign nationals and un-cleared 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.** Classified equipment and material must be stored in an approved secure room, vault, or GSA approved container per reference (c). If a space is operating as “open” storage of classified material/equipment, it must meet all requirements for a secure room/vault. If a space is operating as “closed” storage, all classified material/equipment (i.e., printers, burn bags, and IT assets) must be secured in a GSA approved container, approved secure room/vault, or under the direct control of a cleared individual. Access doors to secure rooms/vaults will be locked with an approved GSA security lock, such as a CDX-09, when not manned by cleared U.S. personnel. Sargent & Greenleaf 8077 locks can only be used on water-tight doors after a waiver/exception for their use has been approved.

   c. **Vault/Open Storage Standards.** Commands will identify all spaces that will be used for storing, handling, and processing classified documents, media, and equipment. Upon identifying these spaces, ensure that all open storage secure room requirements are met. If these requirements cannot be met, job orders will be submitted to have appropriate issues resolved during the next major availability and/or submit a waiver/exception to the Deputy Under Secretary of the Navy for Plans/Policy/Over-sight and Integrations Office.
d. Classified Material Handling. Commands must follow DoD and Navy regulations in the proper handling of classified material. Commands will develop procedures to ensure the proper protection of classified material when not in the direct control of cleared personnel. Per reference (c), use of classified coversheets and training on handling of classified material is required. Commands are required to develop a security training and education program that includes training personnel on classified material handling and marking of all classified material, equipment, and media.

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

f. 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 on file, and need-to-know. The CSM will ensure that this process is completed and updated as required, by verifying information in the Joint Personnel Adjudication System (JPAS).

(1) Additional fields in JPAS, such as IT designation levels and investigation type (National Agency Check with Local Agency Check and Credit Check (NACLC), Single Scope Background Investigation (SSBI), etc.) will be completed in their entirety for all personnel, regardless of security clearance level.

(2) For access to IS, personnel requesting access must be vetted by the CSM. This is done by verifying clearance/access in JPAS and signing the portion of the System Access and Authorization Request-Navy (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.

g. Unauthorized Wireless Devices. All commands must ensure that government and personal wireless devices are not connected to classified networks. These items include, but are
not limited to smart phones, tablets, e-readers, or personal laptops with or without Bluetooth or Wi-Fi capabilities. These items are not allowed into spaces that process or store classified information. All commands, ashore and afloat, must establish a local instruction that covers proper storage and use of Portable Electronic Devices (PEDs) and educate the workforce on that policy. Command-approved devices, such as digital cameras used and controlled for official use, must be approved and designated in writing.

h. Security Incident Handling Procedures. Security incidents must be reported as soon as they are discovered. Incidents must be properly investigated and the necessary actions must be taken to negate or minimize the adverse effects of an actual loss or unauthorized disclosure of classified information. Actions must also be taken to preclude recurrence through a security education and awareness program, and a robust Command Security Instructions. In cases where compromise has been ruled out and there is no adverse effect on national security, a resolution of an incident should be handled at the lowest appropriate level. All security incidents involving classified information shall involve a security inquiry or preliminary inquiry, a security investigation, or both.

i. Visitor Control. Security for commands begins at either the brow, entry control point (ECP), or quarterdeck (QD). Command personnel/watches are to verify the credentials of all non-command personnel at every request for access and personnel requiring escort who do not meet clearance requirements. Commands/contractors/agencies shall submit visit requests to the Commanding Officer who will then grant approval or disapproval for classified visits by individuals to the command. The DoD authoritative source for managing visit requests is the Joint Personnel Adjudication System (JPAS). All other companies or agencies must send an official request via facsimile (fax) or an encrypted (if applicable) email to the Commanding Officer, or his/her security representative.

(1) Visitors. Visitors requiring access to unclassified areas of a command will be vetted by using JPAS list or a valid access list (VAL) provided to the command by the local security authority (i.e., base or region). Visitors requiring access to classified areas that do not have a validated clearance will be escorted at all times, and the classified spaces will be sanitized prior to entry of the visitor.
(2) Controlling Personnel. Command access will be closely monitored, controlled, and documented by watchstanders/staff. The Officer of the Deck (OOD) or security representative is responsible for validating visitor credentials against the daily JPAS list and the VAL. A visitor log will be maintained at the QD/ECP to document all visitors, regardless of military rank or civilian title. The log will document the visitor’s: (1) name, (2) signature, (3) command/company, (4) date, (5) badge number, and (6) time in/out. All visitors will receive a badge that will clearly identify them as “Escort Required” or “Unescorted”. Badges will be displayed at all times and worn above the waist. Badges will be numbered for control purposes and inventoried at the watch turnover with oncoming Staff Duty Officer or security representative. Lost badges will be reported immediately.

(3) Visitor Logs. Ensure visitor control logs are utilized for all visiting personnel not on the command access control list and entering a space in which processing or storing of classified material takes place. To maintain a historical record of personnel entering the space, a visitor Control Log or an Automated Electronic Access Control System may be used.
CHAPTER 7: ORGANIZATIONAL BEHAVIOR

1. Discussion. Operational behavior is how the network is treated by all privileged and authorized users, and is a direct reflection of command culture as it relates to CS. As the DoD requires annual CS Awareness Training for all hands, it is clear that CS compliance is an all-hands effort. To this end, NIOC NBTs assess and evaluate operational behavior compliance during both CSICP Stage II TAVs (via a separate NBT Assessment report), and as part of FLTCYBERCOM OCA’s Stage III CSI.

2. References. Operational behavior involves a combination of adherence to established tactical directives (CTOs, FAMs, Operational Orders, etc.) and best practices. Commands must use VRAM, URL (k), as the Navy’s repository of active Computer Tasking Orders, as well as USCYBERCOM’s website, URL (n), 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 ISSM.

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 captures 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 the proper clearance and/or need-to-know.

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

      (3) Ensure inactive user accounts are disabled or closed within 30 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 an installed default 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.
(5) Ensure that access control lists are written to prevent unauthorized connections from and to the network. (Examples are Web connections are via the Internet Security and Acceleration (ISA) proxy server, or the address of the Navy Cash servers is allowed to make connections to upstream Navy Cash servers for updates).

b. Logs

(1) Network activity log collection and review is a primary source of assessing user behavior. In addition to determining user behavior, logs also provide forensic evidence used by NCDOC in the event of a compromise, spillage/negligent discharge, or other unauthorized event. For these reasons, it is essential that logs are securely stored online for 90 days.

(2) Web proxy (e.g., Microsoft ISA server) is used to collect all web sites visited.

(3) Web server logs collect connections made to internal web servers.

(4) Domain Name Service (DNS) logs collect domain name look-up information for all protocols such as File Transfer Protocol, Telnet, etc.

(5) Router or system logs record information from the router and are configured alongside Access Control Lists.

(6) Event log collection stores hosts such as domain controllers, workstations, or e-mail servers.

c. Human Factors

(1) Inappropriate or unauthorized web browsing and file downloads must be prevented and, if discovered, acted upon immediately. While the Fleet 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) are not to browse the Internet using their administrator accounts. SA 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 ISSM’s responsibility to regularly monitor Internet use on privileged user accounts.

(2) Prevent unauthorized devices (e.g., smart phones, music players, etc.) from connecting to the network. Flash media is prohibited by Navy policy. For commands with HBSS, the DCM can assist in “locking down” USB ports on workstations to prevent unauthorized devices from accessing those ports. Scanning software such as USB Detect can be used to continuously scan for unauthorized removable media devices (RMDs). (Enforcement and adherence requires constant vigilance and repeated user training, with the connection of unauthorized devices presenting a high risk factor).

(3) Discovering the same device used 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 (e.g., hacker penetration) is an obvious high threat factor and requires immediate execution of the Incident Response Plan.

4. Remarks. CS is a readiness issue that impacts our operations in every warfare area, and failure to develop a command climate of responsible network user behavior is a preventable vulnerability that cannot be ignored. Starting from the top, CS is a command-wide responsibility. CO, OICs, and DHs must elevate attention, awareness, training, and accountability of this issue throughout the command. NAVIDFOR stands ready to assist in helping commands institute a strong program and best practices.
# CS Program Administration Spot Check

This enclosure is provided to assist commands in developing their CS Program. This checklist is not all inclusive and must be modified to meet the command’s individual needs.

<table>
<thead>
<tr>
<th></th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is the ISSM appointed in writing?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Do the command’s Secret Material Transfer Agents (SMTAs) follow the procedures from the command’s instruction to transfer classified data to removable media?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Is the command’s Removable Media Representative’s (RMR) list of authorized SIPRNet Media Transfer Agents (SMTAs) up to date?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Do the command’s SMEs and SMTAs follow the procedures from the command’s SOP to transfer data between networks of different classification?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Does the command have an Incident Handling Instruction for electronic media?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Is the ISSM and personnel familiar with the command’s documented cyber incident response plan?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. From a sampling of removable media onboard (at least 25%), are personnel properly labeling removable media?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Do the ISSM and CS personnel maintain an inventory of all classified and unclassified IS equipment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>9. Does the SA maintain a record of SAAR-N forms for all network users, and Privileged Access Agreements (PAAAs) for all Privileged users?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>10. Does the command maintain a list of approved removable storage devices?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Enclosure (1)
11. Has the command developed and implemented two- 
person accountability for classified removable media? [USCC TASKORD 13-0651, CTF 1010 CTO 13-16] 

12. Has the command validated all privileged access network accounts (administrator rights), reduced/deleted non-essential root-level accounts, and revalidated all privileged accounts at least annually? [USCC TASKORD 13-0651, CTF 1010 CTO 13-16] 

13. Is the command’s site ATO current, and does it cover all network enclaves (e.g. SIPRNet and NIPRNet)? Does the command have valid ATO/IATOs for all systems? 

14. Is the drawing of the command’s network topology current? Have all major configuration changes been authorized by the local configuration control board (CCB), cognizant SYSCOM or Platform TYCOM? [DISA STIG NET 0090] 

15. Is there a SOP on how to conduct safe transfers (to include redacting documents) to avoid spillage/negligent discharge? 

Commanding Officer:______________________________

Information Systems Security Manager:_________________
**Network Security Spot Check**

This enclosure is provided to assist commands in developing their CS Program. This checklist is not all inclusive and must be modified to meet the command’s individual needs.

**Date:**

<table>
<thead>
<tr>
<th>Question</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Is the command’s IAVM Vulnerabilities per Asset Weighted Average less than 2.5? (Weighted Average Summary Report Enclosed in enclosure (11)) [CSRM]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2. Is the anti-virus signature file age within seven day periodicity? [DISA STIG]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3. Is the anti-virus software scheduled to scan at least weekly on all network hosts, and are findings of any quarantined files reported to the chain of command? [DISA STIG]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4. Is the command in compliance with current INFOCON requirements? [ALCOM 178-08]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5. Do passwords meet minimum complexity and password age requirements? [ALCOM 178-08]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6. Are default passwords on all network components (e.g., servers, switches, workstations) changed from manufacturer passwords and stored via SF-700 in a container appropriate to the classification? [DISA STIG NET0240]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7. When logging onto the SIPRNet and NIPRNet does a DoD login banner appear? [CTO 08-008A]</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8. Review the last weekly USB Detect scan log. Are anomalies investigated promptly and remedied? How are corrective actions documented. [Command CS Policy &amp; SOPs]</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
9. Are network vulnerability scans conducted at least monthly, and either uploaded to a scan repository VRAM for IT-21 and ONE-NET networks, or retained locally for 90 days for NMCI and excepted networks? [CTO 11-16A]

10. Does the ISSM 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 CS Policy & SOPs]

11. Has the command’s HBSS been properly configured and updated to protect network assets in accordance with DoD and DON guidance? [USCC OPORD 12-1016, SPAWAR HBSS Install Guide]

12. Are data backup procedures per the command’s back-up and recovery instruction? (afloat commands follow PoR guidance) [DoDI 8500.2]

13. Does the command protect against unauthorized removable media usage via HBSS, or have alternate procedures been developed to log all data transfer activity (DTA)? [USCC TASKORD 13-0651, CTF 1010 CTO 13-16]


15. If the command has a DISA-registered Communications Circuit System Designator (CCSD), has the ISSM updated the DoD SNAP database with current CND IPD/IDS data, and assigned IP range? (N/A for afloat commands) [USCC TASKORD 12-1212]

Commanding Officer:__________________________

Information Systems Security Manager:______________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE CO.__________________________
CSWF Spot Check

This enclosure is provided to assist commands in developing their CS Program. This checklist is not all inclusive and must be modified to meet the command’s individual needs.

Date: __________

YES NO

1. Do the ISSM and designated Privileged User personnel have accounts with their applicable Tier 2 vulnerability scan repository (VRAM, VMS)? [NNWC CTO 11-16, 11-16a]  

2. Do the ISSM or ISSO have an account in TWMS to track and report CSWF qualifications and training? [NTD 02-09]

3. Are members of the CSWF documented in TWMS by level and position correctly? [NTD 02-09]

4. Are the administrators of program-managed systems aware of and have access to technical and PM-related websites (i.e., SAILOR 2.1 for SPAWAR-managed systems) [DoDI 8500 series]

5. Are all members of the CSWF fully qualified (e.g., baseline certifications, operating system training, PQS qualified)? [DoD 8140.01]

6. Have all members of the command completed the current DoD Annual CS Awareness Training in E-Learning/TWMS? [SECNAV M-5239.2, DoD 8140.01]

7. Does the command have a training plan in place and does it include CSWF members’ requirements to earn Continued Education Units (CEUs)? [DoD 8140.01]
8. Does the command have a locally generated Cyber Security Workforce Improvement Plan (CS WIP) outlining the command’s plan for training and certifying its workforce? [SECNAV M-5239.2]

9. Do all CSWF members have an Individual Development Plan (IDP)? [SECNAVINST 5239.2, COMNAVIDFORINST 5239.1]

Commanding Officer:______________________________

Information Systems Security Manager:_____________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE CO
Traditional Security Spot Check  
(To be completed by the Command Security Manager)

Date: ________

1. Does the command have a local security instruction that outlines local security policies and procedures? 
   [DoD 5200.01 Series/SECNAV M-5510.36]  
   YES  NO

2. Are the Command Security Manager (CSM) and Top Secret Control Officer (TSCO) appointed in writing by the CO?  
   [DoD 5200.01 Series/SECNAV M-5510.36]  
   YES  NO

3. In observation of the quarterdeck watch(es), does the ship verify the credentials of non-ship force personnel for each request for command access, and escort personnel who do not meet clearance requirements?  
   [DoD 5200.01 Series/SECNAV M-5510.36]  
   YES  NO

4. Are procedures in place to validate clearances and need-to-know for visitors accessing, or with the potential to access, classified spaces?  
   [DoD 5200.01 Series/SECNAV M-5510.36]  
   YES  NO

5. Does the command employ a security education program, developed and implemented by the CSM, to provide continuous training to command personnel on security procedures and classified material handling?  
   [DoDM 5200.01 Series/SECNAV M-5510.36]  
   YES  NO

6. Is the CSM aware of, and employ, proper incident response procedures to respond to a security violation, and are site personnel aware (through the security education program) of reporting procedures?  
   [DoDM 5200.01 Series/SECNAV M-5510.36]  
   YES  NO

7. Has the command completed an annual security self-inspection and corrected/updated the discrepancies (if noted) from the previous self-inspection?  
   [DoD 5200.01 Series/SECNAV M-5510.36]  
   YES  NO
8. Have the CNO checklists been completed for all spaces that store or process classified information (to include all spaces with classified IT equipment, i.e., SIPRNet)? [SECNAV-M 5510.36/CNO MEMO 16 MAR 10]

9. Have certification letters (or waivers/exceptions completed) been signed for all areas where classified information is processed or stored? [SECNAV-M 5510.36/CNO MEMO 16 MAR 10]

10. Are security personnel familiar with the proper techniques and procedures to declassify/redact documents from a higher classification to a lower classification, and know who the Original Classification Authority (OCA) is in their chain of command? [DoDM 5200.01 Series/SECNAV M-5510.36]

Commanding Officer:____________________________

Information Systems Security Manager:______________________

DISCREPANCIES MUST BE CORRECTED IMMEDIATELY AND ACTION TAKEN REPORTED TO THE CO
Afloat/Ashore CS Command Self-Assessment

This enclosure is provided to assist commands in developing their CS Program. This checklist is not all inclusive and must be modified to meet the command’s individual needs.

**Program Administration**

<table>
<thead>
<tr>
<th>Yes</th>
<th>No</th>
</tr>
</thead>
</table>

1. Is command leadership (Commander, Deputy Commander, CO, XO, COS, DHs/ACOS, etc.) fully engaged in the CS program? [CJCSINST 6510.01F]

2. Are all CS personnel assigned/qualified per 8140.01? [DoDDirective 8140.01]

3. Has a full ATO been achieved, and is it current for both NIPRNet and SIPRNet? [DoDINST 8510.01]

4. Does a CS Certification Program exist? [DoDDirective 8140.01]

5. Are Tenant Command MOUs/MOAs in place? (NOTE: MOA/MOU must have tenant commands’ responsibilities and duties clearly defined, to ensure all CS tasks are accomplished).

6. Is a comprehensive IAVM program in place? [CTO 08-05]

7. Has a local incident handling program been developed and exercised semi-annually, including development of an after-action or lessons learned report? [TASKORD 13-0651]

8. Do approved POA&Ms exist for identified vulnerabilities? [DoDINST 8510.01]

9. Are Configuration Management (CM) processes implemented and enforced (including those for the ISSO/ISSM)? [CJCSINST 6510.01F]

10. Are administrators aware of and able to implement STIG requirements? [CNSSINST 1253]
11. Is the security staff properly trained (see Chapter 6 for detailed requirements), allowing for separation of duties with each individual appointed ___ ___

12. Are all appointments in writing and signed by the current CO? [DISA Contributing Factors Guide] ___ ___


14. Are vulnerability management (e.g., scanning and patching) processes consistent and repeatable? How are they verified? [DISA Contributing Factors Guide] ___ ___

15. Have identified vulnerabilities been addressed immediately? [DISA Contributing Factors Guide] ___ ___

16. Configuration Management: Are the PM system baselines consistent with risks identified and accepted by the Designated Approving Authority (DAA) for the PM System? [DISA Contributing Factors Guide] ___ ___

17. Are SOPs/Programs available for, at a minimum, the following areas: [DISA Traditional Security STIGs] ___ ___
   - Handling of suspected system compromise (e.g., NCDOC incident response procedures)
   - INFOCON procedures and policies
   - Implementing password change policies
   - Purging of storage media prior to turn-in, disposal, or proper re-use
   - Use of screensavers/unattended terminals
   - Virus detection and scanning
   - Building Floor Plans (Identify areas that process/store classified information for afloat units)
   - Access Control System information (Router ACL)
   - Emergency Action Plan
   - Data Backups
   - Electronic Spillage/Negligent Discharge
### Operational Behavior (Classified and Unclassified)

**YES**  **NO**

#### Configuration

1. Do Shares have the correct permissions (all shares should have AUTHENTICATED USERS at a minimum)?  
   [DISA STIG]

2. If a proxy server is used (i.e., Microsoft Internet Security and Acceleration (ISA) Server), is there evidence of it being bypassed by users?  
   [DISA STIG]

3. Are inactive accounts disabled after 30 days of inactivity per NNWC CTO 13-15?

4. Are inactive accounts deleted after 45 days of inactivity per NNWC CTO 13-15?

5. Have default passwords been changed for all IS accounts/devices (WARNING: Follow PoR or vendor guidance to change defaults) [CJCSINST]

6. If a proxy server is utilized, is logging turned on and stored for 90 days? Are logs reviewed and actions taken or discrepancies noted?  
   [DISA STIG]

7. If a web server is utilized, is logging turned on and stored for 90 days? Are logs reviewed and actions taken or discrepancies noted?  
   [DISA STIG]

8. On the DNS server, is logging turned on and stored for 90 days? Are logs reviewed and actions taken or discrepancies noted?  
   [DISA STIG]

9. On the router, is logging turned on and stored for 90 days? Are logs reviewed and actions taken or discrepancies noted?  
   [DISA STIG]
10. Is there any indication of misuse detected within any logs or in the packet data? Is action taken for any misuse noted? [DISA STIG]
Human Factors

1. Have unauthorized devices (e.g., iPod, cell phones, etc.) been connected to unclassified networks since the last self-assessment? [DISA STIG]

2. Is there evidence of users visiting inappropriate websites? [DISA STIG]

3. Is the hardware inventory detailed enough to allow an administrator to physically locate a device on the network? [DISA STIG]

4. Have all patches released by the PoR been applied? [DISA STIG]

5. Are privileged access accounts configured to adhere to the principle of “separation of privileges” (i.e., disable web browsing, no exchange mailbox)? [TASKORD 14-0185]

6. Is the ship/site uploading scans to VRAM or VMS monthly? [TASKORD 13-0670]

High Threat Factors

1. Have unauthorized devices (e.g., iPods, smartphones, etc.) been connected to SIPRNet since the last self-assessment? [DISA STIG]

2. Has any single RMD been used on both NIPRNet and SIPRNet (if yes, this is a Cross Domain violation, which is an NCDOC reportable incident)? [TASKORD 14-0185]

3. Are Antivirus scans being accomplished across the entire network at least weekly, and are the logs of those scans reviewed by CSWF personnel? [DISA STIG]

4. Are CSWF personnel reviewing security logs and HBSS alerts daily, and taking prompt, documented corrective action when discrepancies are found? [DISA STIG]

5. Is there any indication of compromise detected within any logs or packet data? [DISA STIG]
Network Infrastructure

1. Are unused and/or unauthorized NETSEC Ports turned off? [DISA STIG]
2. Are any of the Routers or Switches missing security patches? [DISA STIG]
3. Are all Firewalls configured to the appropriate STIGs? [DISA STIG]
4. Are all Routers and Switches configured to the appropriate STIGs? [DISA STIG]
5. Anti-virus configured per vendor or PoR guidance, including periodic scans? [DISA STIG]
6. Have the ISSM and HBSS administrator disabled any unused and/or unauthorized USB ports? [DISA STIG]
7. Is a list of command-approved Removable Media Devices (RMD) signed by the current CO, such as authorized USB drives, available and reviewed regularly for changes? [TASKORD 13-0651]
8. Have the administrators verified that Share Drive permissions are disabled by default? [DISA STIG]
9. Is Windows Active Directory configured per DISA STIGs? [DISA STIG]
10. Is the Warning Banner displayed on all network equipment IAW CTO 08-05A?
11. Are administrator account passwords being properly managed? Is there an SF-700 (stored in an approved GSA container) for each SA account and system/device password? [DISA STIG]
12. Are administrators running Anti-Virus detection and scans at least every 7 days? Are administrators checking for new anti-virus signatures at least weekly? [DISA STIG]
13. **Intrusion Detection System (IDS) (if installed):**
   Does the ship maintain IDS Information and drawings if available? [DISA STIG]

14. **Has the site properly aligned with the Computer Network Defense Service Provider CNDSP (i.e., NCDOC) and leverages those capabilities?** [DISA Contributing Factors Guide]

15. **Has an internal and/or external Network Intrusion Detection System (NIDS) been deployed and is the CNDSP monitoring?** If external, is the NIDS located at the enclave boundary to the wide area network and monitored by an accredited Tier II CNDSP. If no, explain: (N/A for afloat, NIDS is located at Fleet NOC) [DISA STIG]
Traditional Security

1. Does a Protected Distribution System (PDS) Certification Letter and applicable system drawing/diagram exist? (N/A for afloat) [DISA STIG]  

2. Does wall jack protection exist (e.g. approved lock box with approved lock (Sargent & Greenleaf 8077), or port security (802.1x), or secure room for all classified network drops)? [DISA STIG]  

3. Do uncleared personnel have access to classified spaces (including temporary personnel such as Food Service Attendants)? [DISA STIG]  

4. Are space designation letters completed for all required areas and signed by the Commanding Officer (Secure Room, Control Access Areas, and Restricted Access Areas)? [DISA STIG]  

5. Does an approved Emergency Action Plan exist to include destruction of classified material? [DISA STIG]  

6. Do visitor security procedures exist to allow cleared visitors authorized access to classified spaces? [DISA STIG]  

7. Do foreign national procedures exist to restrict foreign nationals from NOFORN information? [DISA STIG]  

8. Spot check three (3) random spaces for the following: [DISA STIG]  
   a. CAC left unattended  
   b. Unlocked, unattended IS workstations  
   c. Unauthorized wireless device  

9. Does a Key and Lock Program exist? Is there a written local policy in place? [DISA STIG]  

10. Does a command physical security plan exist, to include all local security policies and procedures? [DISA STIG]
11. Are all Vaults and Safes properly certified (e.g., GSA-approved containers)? [DISA STIG]

12. Do procedures for end of work day security checks exist (SF-701 checksheets for each space that processes and stores classified information)? [DISA STIG]

13. Are IDS installed for secure spaces, are they inspected and operationally tested regularly? [DISA STIG]

14. Do policies and procedures exist for the proper handling of classified material? [DISA STIG]


16. Are DD Form 2056 attached to all telephones subject to COMSEC telephone monitoring? [DISA STIG]

17. Are copies of DD Form 254 on file for all contracts in which contractors have access to classified information? [DISA STIG]

18. Has the correct investigation been submitted on all personnel based on their position sensitivity and IT level? [DISA STIG]

19. Do SOPs/procedures exist for the following: [DISA STIG]

   - Personnel Security Files (Military and Civilian)
   - Contractor Security Files and all applicable DD 254s
   - Mil/Civilian PD Designations (IT designations)
   - Courier Card/Letter Program
   - Periodic Reinvestigations
   - Classified wrapping/transmission
   - Classified meetings
   - Need-to-know/Non-Disclosure Agreement
   - JPAS: Personnel with lapsed or denied clearances
Cyber Zone Inspection Checklist

SPACE NAME/DESIGNATION: ___________________________ DATE: ______

NAME OF ZONE INSPECTOR: ________________________________

NAME/DIVISION OF SPACE OWNER: ___________________________

NOTE: This zone inspection encompasses physical security and IT security checks for workspaces. Recommended rates: IT/CT, or PHYSEC. Format derived from COMNAVSURFORINST 3120.1.

SAT/UNSAT

1. CLASSIFIED SPACES: Does the space meet the requirements for the level of information being processed per DoD Manual 5200.01, Volume 3, enclosure 3? Is the space designated as (circle one):

- Controlled Access Area (CAA)
- Restricted Access Area (RAA)
- Open Secret Storage Area (OSS)

2. CLASSIFIED SPACES: Are classified documents, media, and equipment that are not under the personal control and observation of an authorized person being stored in a GSA-approved security container when not in use?

3. CLASSIFIED SPACES: Are screens for classified systems able to be viewed from outside the space?

4. CLASSIFIED SPACES: Is an access control list, SF-701 (activity security checklist), and SF-702 (security container check sheet) posted and properly filled out?

5. CLASSIFIED SPACES: If the space is a CAA, RAA, or OSS, is it protected with a GSA-approved lock (i.e., CDX-09)?
6. CLASSIFIED SPACES: Does the space allow appropriate visual monitoring of access, or access control for authorized personnel (i.e., cypher lock)?

7. CLASSIFIED SPACES: Are information processing systems clearly labeled with their classifications?

8. CLASSIFIED SPACES: Is there a minimum of one meter separation between classified and unclassified information processing systems? [TEMPEST]

9. CLASSIFIED SPACES: If the space is a CAA, RAA, or OSS, are there unauthorized Personal Electronic Devices (PEDs) (i.e., smart phones, tablets, personal laptops, etc.)?

10. ALL WORKSPACES: Are there unattended Common Access Cards (CAC) or other smart card credentials controlling access to information systems?

11. ALL WORKSPACES: Are any sensitive-but-unclassified material, such as PII, left unprotected from unauthorized disclosure?

12. ALL WORKSPACES: Do the serial numbers/asset tags of information processing systems in the space match the hardware inventory? (e.g., desktop/laptop workstations)

Commanding Officer: ________________________________

Executive Officer: ________________________________

Space Owner Department Head: ______________________

Information Systems Security Manager: ______________________

Command Security Manager: ______________________________

Zone Inspector: ________________________________
CO’s CS Questionnaire

This enclosure is provided to assist commands in developing their CS Program. This checklist is not all inclusive and must be modified to meet the command’s individual needs.

This is a self-assessment questionnaire to provide COs and their ISSMs a starting point for determining the health and status of the command’s network. This is a good tool to use when turning over ISSM duties, establishing/improving a CS program, or after a change of command to “rudder check” the command’s CS program.

PHYSEC and Program Administration

1. Is our Physical Distribution System certified and are the documents available for viewing by the inspection team? If we don’t have a Physical Distribution System, do we have an approved CNO waiver to operate without one? (N/A for afloat units)

2. Do we have a command security training and education program? Are we instructing our personnel on proper handling and marking of classified material?

3. Is our CSWF properly appointed in writing (ISSM, ISSOs, Privileged Users, etc.)? Have they completed all required training and CEU requirements to retain certification?

4. Have we verified that Privileged Access Users (SA) have signed IS Privileged Access Agreements (PAAs)?

5. Have all personnel completed the mandatory annual CS training by the required due date? If not, what is the plan for getting us there?

6. Do we have copies of all users SAAR-N forms and annual CS training certificates (or FLTMPS report)?

7. Have all command personnel received OPSEC training and when was it completed?
Network Review

1. Does the Network Topology Diagram accurately reflect our current architecture and is it available for review? Are we submitting any changes to the SYSCOM PMs, NAVIDFOR/IDFOR, and/or Platform TYCOM?

2. Do we really know the actual number of devices connected to our network? Really know? [Hint: Your ISSM should have run RETINA, a discovery tool, to find this out.]

3. Are our Access Control Lists (ACLs) for our routers, switches, and firewalls ready for an inspector to review? Are all privileged access passwords contained in SF-700 envelopes and stored in a GSA-approved security container?

4. Which CND tactical directives are we having trouble complying with? (e.g., CTOs, NTDs, FRAGOs, OPORDs, etc.) What are we doing about it? Who have we contacted for help?

5. Do we have signed Memorandums of Agreement or Understanding with all tenant commands connected to our network? If we are a tenant command, do we have a copy of our agreement?

6. When was the last time a complete CS inventory was conducted? [Hint: Should be semi-annual, full hardware and software validation.]

7. Is our site ATO/IATO within periodicity, and have we completed all POA&M items from the last accreditation?

Vulnerability Scans

1. On what date was the last monthly network vulnerability scan conducted? What were the results? What was done to correct deficiencies noted?

2. Are you reviewing the network scan results on a monthly basis? Who validates that noted vulnerabilities have been corrected? Is this a formalized, documented process?

3. What vulnerabilities were identified that we were unable to patch or mitigate?
4. Do we have a POA&M to correct those vulnerabilities that we have the ability to correct?

**Previous Inspections**

1. Do we have documentation (out-brief, list of findings, or POA&M) of the following previous inspections?
   
   a. CSI Stage I (ISIC Admin Review)
   
   b. CSI Stage II (TAV)
   
   c. CSI Stage III (CSI/CCRI)
   
   d. Board of INSURV IS Material Inspection (MI)
   
   e. TYCOM Material Inspection (MI)

2. Have we corrected all vulnerabilities found from the inspection? If not, why not and what are we doing to get outside SYSCOM and TYCOM assistance?

3. Do we have a mitigation plan in place for those findings that cannot be immediately corrected?

**Points of Contact**

1. Who are your points of contact at our ISIC, our Platform TYCOM, and ID TYCOM?

2. When was the last time you communicated with them?
Minimum Set of Periodic Reports

This enclosure is provided to assist commands in developing their CS Program. This checklist is not all inclusive and must be modified to meet the command’s individual needs.

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 ISSM/ISSO, with copies forwarded as directed by higher authority.

1. Irregular Reports

   a. 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 CS discrepancies (per DISA STIGs or IAVM security patches) can be noted as exceptions when the SOVT is completed. This is important, since PoR 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 systems compliant with CS regulations. These noted discrepancies will not pass as CSI or CCRI waivers, but will assist in command awareness of CS requirements and as appropriate, these findings will be attributed to PoR scoring (for ships) and not the Ship’s Force responsible grade.

   b. Cyber Incident Reports. In the event that a cyber incident occurs at the command, CS personnel shall provide timely initial and regular update reports to the command team on actions taken and how the incident affects the command’s CS posture and overall mission readiness. Incident reports are handled per reference (m) and routed through the chain of command for approval and situational awareness.
2. Semi-annual Reports

   a. C&A. Review the status of all command systems’ 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. **A sample report is provided as Enclosure (9) to this handbook.**

   b. Network Configuration and Inventory. Review and update the command’s network diagrams. Drawings should be current and include any changes to the network configuration that have occurred in the previous 6 months. These configuration changes will be reported to the appropriate PoR, NAVIFOR, and platform TYCOM. Accurate network diagrams are critical to successful network management and are required for ATO renewal and CSIs. A validation of all hardware and software inventory shall be conducted and reported as an addendum to the topology report.

3. Monthly Reports

   a. Cyber Training Report. Review the status of required CS training for all CSWF personnel. Additionally, all hands are required to complete on-line CS Awareness Refresher training within the last year. Additionally, personnel in positions of trust (SAs, command ISSM/ISSO, etc.) shall be certified at the required level of CSWF training or must have submitted waivers. **A sample report is provided as enclosure (10) to this handbook.**

   b. Vulnerability Management (VM) Detailed Report. Review the detailed status of the command’s compliance with all identified CS vulnerabilities as reported in the VRAM website URL (k), which is also reviewed in detail by the command’s ISIC and TYCOM. This report includes results of periodic network vulnerability scans and reporting compliance (scanning all assets within prescribed periodicity) and audit status (total number of open vulnerabilities, their severity, and percentage of those vulnerabilities that are identified by the PoR as within the command’s ability to remediate). In reviewing this detailed report, special attention shall be taken to ensure that all computers/systems on the network are being scanned, and that “site-owned” vulnerabilities are being tracked to closure. **A sample report is provided as enclosure (11) to this handbook.**
4. Weekly Reports

   a. CS Status Report. The ISSM shall provide a report that gives an overview of the command’s CS posture in a “dashboard” format, to include the following elements at a minimum: CND suite status (e.g., HBSS, intrusion detection/prevention systems, etc), Anti-virus status, protection against unauthorized removable media (i.e., USB Detect scans), compliance with tactical directives, and operational updates. The CS Status Report provides leadership with all the data required to ensure that the command is maintaining a proper level of cyber readiness. It is recommended that ISSMs color-code this report for ease of readability and highlight key issues to senior organizational leadership. A sample report is provided as enclosure (12) to this handbook.

5. Sample Reports. The following enclosures provide templates for the periodic reports delineated above. These templates are provided to assist Command’s in developing their CS Program. These templates are not all inclusive and should be modified to meet the command’s individual needs. Existing report formats need not be changed as long as they provide the appropriate information.
## TEMPLATE: Certification and Accreditation Report
(Semiannual)

<table>
<thead>
<tr>
<th>System Name</th>
<th>ATO Type (circuit, system, application, site, etc)</th>
<th>Last ATO Date</th>
<th>ATO Exp Date (begin renewal actions NLT 180 days prior to exp)</th>
<th>Action Status (Obtained from eMASS if submitted, otherwise cite local actions prior to C&amp;A submission)</th>
<th>Current Action Due Date</th>
<th>Next Action and estimated completion date</th>
<th>ISSM Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>USS [Ship Name]</td>
<td>Site</td>
<td>May 2011</td>
<td>May 2014</td>
<td>C&amp;A package submitted to ISIC</td>
<td>March 2014</td>
<td>Collaboration, April 2014</td>
<td>On track to obtain renewal prior to exp date</td>
</tr>
</tbody>
</table>

(Other systems site is responsible for per ODAA – NOTE afloat is only responsible for SITE ATO)

---

ISSM: _________________ DIVO: _________________ DH: _________________ XO: _________________ CO: _________________
**TEMPLATE: Cyber Training Report**  
(Monthly)

**CSWF Training and Certification Status**

<table>
<thead>
<tr>
<th>Name</th>
<th>Position</th>
<th>Rqd IA Lvl</th>
<th>Qual Status</th>
<th>Due Date</th>
<th>Waiver Req Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: ITCS Jones</td>
<td>ISSM</td>
<td>ISSM</td>
<td>90% compl</td>
<td>Dec 2014</td>
<td>N/A</td>
</tr>
<tr>
<td>Example: IT2 Kelly</td>
<td>Sys Admin</td>
<td>IAT Level II</td>
<td>50% compl</td>
<td>Mar 2014</td>
<td>6-mo extension approved by NAVIFOR, dtd DDMMYY</td>
</tr>
</tbody>
</table>

**Authorized User Training Status**

<table>
<thead>
<tr>
<th>Training</th>
<th>Data Source</th>
<th>Total # of Users</th>
<th>Training Completed</th>
<th>Percentage Completed</th>
<th>Due Date</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Example: Annual CS Refresher Training</td>
<td>FLT MPS</td>
<td>175</td>
<td>172</td>
<td>98%</td>
<td>Feb 2014</td>
<td>3 users not completed training; accounts disabled</td>
</tr>
</tbody>
</table>

Local command training efforts as directed (i.e., divisional/crew training)

| ISSM: ____________________ | DIVO:__________________ | DH: __________________ | XO: __________________ | CO: __________________ |

Enclosure (10)
### Unclassified Networks

#### Scanned Asset Summary

Derived from Vulnerability Remediation Asset Manager (VRAM) Site Workspace.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Last Scan</th>
<th>Days Since Last Scan</th>
<th>Total Assets</th>
<th>Assets (Current)</th>
<th>Assets (Outdated)</th>
<th>Invalid Scans</th>
<th>Percent Scanned</th>
<th>Scan Integrity</th>
<th>Retina Version</th>
<th>ACAS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS V1 WIN 7</td>
<td>2015-08-24</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>100%</td>
<td>0%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>CND-OSE 1.2</td>
<td>2015-08-22</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>ISNS with COMPOSE 3.0.X</td>
<td>2015-08-23</td>
<td>4</td>
<td>161</td>
<td>161</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>Navy Cash 1.4.7</td>
<td>2015-08-22</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>NIAPS 2.x</td>
<td>2015-08-22</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>NSIPS Web Afloat 1.3</td>
<td>2015-08-22</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>NTCSST Patriot</td>
<td>2015-08-22</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>Unassigned</td>
<td>2015-08-23</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
</tbody>
</table>

#### Site Vulnerability Summary

Derived from Vulnerability Remediation Asset Manager (VRAM) Site Workspace.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Total Assets</th>
<th>IAV Compliance</th>
<th>Severity Category Compliance</th>
<th>Outdated Assets</th>
<th>Unique Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>A   B   T</td>
<td>Total</td>
<td>% Site Owned</td>
<td>I   II  III  IV</td>
</tr>
<tr>
<td>AIS V1 WIN 7</td>
<td>1</td>
<td>0    0    0</td>
<td>0</td>
<td>0%</td>
<td>0   0  0  0</td>
</tr>
<tr>
<td>CND-OSE 1.2</td>
<td>2</td>
<td>37   4    0</td>
<td>41</td>
<td>76%</td>
<td>14  27 0 0</td>
</tr>
<tr>
<td>ISNS with COMPOSE 3.0.X</td>
<td>161</td>
<td>191   33   2</td>
<td>226</td>
<td>75%</td>
<td>140 86 0 0</td>
</tr>
<tr>
<td>Navy Cash 1.4.7</td>
<td>2</td>
<td>31   1    0</td>
<td>32</td>
<td>69%</td>
<td>18  14 0 0</td>
</tr>
<tr>
<td>NIAPS 2.x</td>
<td>1</td>
<td>68   9    0</td>
<td>77</td>
<td>3%</td>
<td>39  38 0 0</td>
</tr>
<tr>
<td>NSIPS Web Afloat 1.3</td>
<td>1</td>
<td>21   1    0</td>
<td>22</td>
<td>23%</td>
<td>13  9  0 0</td>
</tr>
<tr>
<td>NTCSST Patriot</td>
<td>1</td>
<td>12   3    0</td>
<td>15</td>
<td>40%</td>
<td>15  0  0 0</td>
</tr>
<tr>
<td>Unassigned</td>
<td>6</td>
<td>31   7    2</td>
<td>40</td>
<td>0%</td>
<td>35  5  0 0</td>
</tr>
</tbody>
</table>
### Weighted Average Summary

Calculated from Scanned Asset and Site Vulnerability Summaries.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Total Assets</th>
<th>I</th>
<th>II</th>
<th>III</th>
<th>IV</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS V1 WIN 7</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CND-OSE 1.2</td>
<td>2</td>
<td>14</td>
<td>27</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>ISNS with COMPOSE 3.0.X</td>
<td>161</td>
<td>140</td>
<td>86</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Navy Cash 1.4.7</td>
<td>2</td>
<td>18</td>
<td>14</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NIAPS 2.x</td>
<td>1</td>
<td>39</td>
<td>38</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NSIPS Web Afloat 1.3</td>
<td>161</td>
<td>140</td>
<td>86</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>NTCSS Patriot</td>
<td>1</td>
<td>15</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Unassigned</td>
<td>6</td>
<td>35</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>175</strong></td>
<td><strong>274</strong></td>
<td><strong>179</strong></td>
<td><strong>0</strong></td>
<td><strong>0</strong></td>
</tr>
</tbody>
</table>

Weighted Average per Asset:

- Weighted Average Total = ((CAT I Vulnerabilities per Asset * 10) + (CAT II Vulnerabilities per Asset * 4) + (CAT III Vulnerabilities per Asset * 1)) / (10+4+1)

**Weighted Average Calculation:**

- CAT I Vulnerabilities per Asset = Total CAT I / Total Assets
- CAT II Vulnerabilities per Asset = Total CAT II / Total Assets
- CAT III Vulnerabilities per Asset = Total CAT III / Total Assets
- Weighted Average Total = ((CAT I Vulnerabilities per Asset * 10) + (CAT II Vulnerabilities per Asset * 4) + (CAT III Vulnerabilities per Asset * 1)) / (10+4+1)
- The color grading criteria is: GREEN < 2.5; YELLOW >= 2.5; RED >= 3.5
### Classified Networks

**(NOTE: The inclusion of classified vulnerability scan results will require classification markings and protection at the appropriate level.)**

#### Scanned Asset Summary

Derived from Vulnerability Remediation Asset Manager (VRAM) Site Workspace.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Last Scan</th>
<th>Days Since Last Scan</th>
<th>Total Assets</th>
<th>Assets (Current)</th>
<th>Assets (Outdated)</th>
<th>Invalid Scans</th>
<th>Percent Scanned</th>
<th>Scan Integrity</th>
<th>Retina Version</th>
<th>ACAS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>AIS V1 WIN 7</td>
<td>2015-08-24</td>
<td>2</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>100%</td>
<td>0%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>CND-OSE 1.2</td>
<td>2015-08-22</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>ISNS with COMPOSE 3.0.X</td>
<td>2015-08-23</td>
<td>4</td>
<td>161</td>
<td>161</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>Navy Cash 1.4.7</td>
<td>2015-08-22</td>
<td>5</td>
<td>2</td>
<td>2</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>NIAPS 2.x</td>
<td>2015-08-22</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>NSIPS Web Afloat 1.3</td>
<td>2015-08-22</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>NTCSS Patriot</td>
<td>2015-08-22</td>
<td>5</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
<tr>
<td>Unassigned</td>
<td>2015-08-23</td>
<td>4</td>
<td>6</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>100%</td>
<td>100%</td>
<td>5.19.11.2910</td>
<td>4.8.1</td>
</tr>
</tbody>
</table>

#### Site Vulnerability Summary

Derived from Vulnerability Remediation Asset Manager (VRAM) Site Workspace.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Total Assets</th>
<th>IAV Compliance</th>
<th>Outdated Assets</th>
<th>Unique Findings</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>A</td>
<td>B</td>
<td>T</td>
<td>Total</td>
</tr>
<tr>
<td>AIS V1 WIN 7</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>CND-OSE 1.2</td>
<td>2</td>
<td>37</td>
<td>4</td>
<td>41</td>
</tr>
<tr>
<td>ISNS with COMPOSE 3.0.X</td>
<td>161</td>
<td>191</td>
<td>33</td>
<td>226</td>
</tr>
<tr>
<td>Navy Cash 1.4.7</td>
<td>2</td>
<td>31</td>
<td>1</td>
<td>32</td>
</tr>
<tr>
<td>NIAPS 2.x</td>
<td>1</td>
<td>68</td>
<td>9</td>
<td>77</td>
</tr>
<tr>
<td>NSIPS Web Afloat 1.3</td>
<td>1</td>
<td>21</td>
<td>1</td>
<td>22</td>
</tr>
<tr>
<td>NTCSS Patriot</td>
<td>1</td>
<td>12</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>Unassigned</td>
<td>6</td>
<td>31</td>
<td>7</td>
<td>40</td>
</tr>
</tbody>
</table>
### Weighted Average Summary

Calculated from Scanned Asset and Site Vulnerability Summaries.

<table>
<thead>
<tr>
<th>System Name</th>
<th>Total Assets</th>
<th>Severity Category Compliance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>I</td>
</tr>
<tr>
<td>AIS V1 WIN 7</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>CND-OSE 1.2</td>
<td>2</td>
<td>14</td>
</tr>
<tr>
<td>ISNS with COMPOSE 3.0.X</td>
<td>161</td>
<td>140</td>
</tr>
<tr>
<td>Navy Cash 1.4.7</td>
<td>2</td>
<td>18</td>
</tr>
<tr>
<td>NIAPS 2.x</td>
<td>1</td>
<td>39</td>
</tr>
<tr>
<td>NSIPS Web Afloat 1.3</td>
<td>1</td>
<td>13</td>
</tr>
<tr>
<td>NTCSS Patriot</td>
<td>1</td>
<td>15</td>
</tr>
<tr>
<td>Unassigned</td>
<td>6</td>
<td>35</td>
</tr>
<tr>
<td><strong>TOTAL</strong></td>
<td><strong>175</strong></td>
<td><strong>274</strong></td>
</tr>
</tbody>
</table>

Weighted Average per Asset: 1.3165714

- **ISSM:** ____________  **DIVO:** ____________  **DH:** ____________  **XO:** ____________  **CO:** ____________

**Weighted Average Calculation:**

- CAT I Vulnerabilities per Asset = Total CAT I / Total Assets
- CAT II Vulnerabilities per Asset = Total CAT II / Total Assets
- CAT III Vulnerabilities per Asset = Total CAT III / Total Assets
- Weighted Average Total = ((CAT I Vulnerabilities per Asset * 10) + (CAT II Vulnerabilities per Asset * 4) + (CAT III Vulnerabilities per Asset * 1)) / (10+4+1)
- The color grading criteria is: **GREEN < 2.5**; **YELLOW >= 2.5**; **RED >= 3.5**
NOTE: The inclusion of classified vulnerability scan results will require classification markings and protection at the appropriate level.

### Template: CS Status Report
(Daily/Weekly)

<table>
<thead>
<tr>
<th></th>
<th>NIPR ISNS COMPOSE</th>
<th>SIPR ISNS COMPOSE</th>
<th>AIS V1 WIN 7</th>
<th>NIAPS v2.X</th>
<th>Other Networks (add more columns as necessary)</th>
</tr>
</thead>
<tbody>
<tr>
<td># of Servers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of Workstations</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Information Assurance Vulnerability (IAV) Scans
*Derived from Vulnerability Remediation Asset Manager (VRAM) Site Workspace dashboard*

<table>
<thead>
<tr>
<th>Aspect</th>
<th>NIPR ISNS COMPOSE</th>
<th>SIPR ISNS COMPOSE</th>
<th>AIS V1 WIN 7</th>
<th>NIAPS v2.X</th>
<th>Other Networks (add more columns as necessary)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Patches/FAMs/STIGs release</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(In last 48 hours have been successfully applied to all machines.)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Days Since Last Scan</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(from reporting status review)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scan Integrity</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(from reporting status view)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Scanner Version Used</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(from reporting status view)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>% of site-owned vulnerabilities</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(audit status graph under Site Summary)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong># of outdated Antivirus</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(from audit status view)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong># of Agent.BTZ findings</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(from audit status view)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>% of assets manually validated as fully patched</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><em>(physical sampling of network assets to verify the weekly patching process was successful – see the NAVIFOR CSRMS,)</em></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Host Based Security System HBSS</strong>&lt;br&gt;Derived from HBSS &quot;FLTCYBERCOM Executive Dashboard&quot;</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># Confirmed Intrusion Prevention (IPS) Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># Confirmed Data Link Protection Events</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># Point Product Non-Compliant Assets</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td># of detected rogue systems</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Antivirus Scanning</strong>&lt;br&gt;Derived from installed Antivirus managed suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Automated Virus Scan</td>
</tr>
<tr>
<td># of Assets Successfully Scanned</td>
</tr>
<tr>
<td># of A/V findings (quarantined/deleted)</td>
</tr>
<tr>
<td>If virus found, cite file name/virus signature as reported by scanner</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Removable Media Devices (i.e., USB Detect)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Scan/Inspection</td>
</tr>
<tr>
<td># Scanned/Inspected</td>
</tr>
<tr>
<td># Authorized Use</td>
</tr>
<tr>
<td># Unauthorized Use</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Back-ups</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Completed Date</td>
</tr>
<tr>
<td>Tested Date</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Account Management</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td># Privileged Accounts&lt;br&gt;(Including Default and Service Accounts)</td>
</tr>
<tr>
<td>Date of last account validation&lt;br&gt;validate privileged users as mission-essential only, lock</td>
</tr>
<tr>
<td>CSWF (CSWF) Status</td>
</tr>
<tr>
<td>---------------------</td>
</tr>
<tr>
<td>Current</td>
</tr>
<tr>
<td>90-Day Projection</td>
</tr>
<tr>
<td>120-Day Projection</td>
</tr>
</tbody>
</table>

ISSM: ____________  DIVO: ____________  DH: ____________  XO: ____________  CO: ____________
The following is an excerpt from the SANS Institute, a cooperative, open-source research and education organization founded in 1989 that has become one of the most trusted and largest sources of IS training and research in the world. SANS is frequently referenced by the U.S. government as an authoritative source for industry best practices.

**Critical Security Controls for Effective Cyber Defense**

Over the years, many security standards and requirements frameworks have been developed in attempts to address risks to enterprise systems and the critical data in them. However, most of these efforts have essentially become exercises in reporting on compliance and have actually diverted security program resources from the constantly evolving attacks that must be addressed. In 2008, this was recognized as a serious problem by the U.S. NSA, and they began an effort that took an "offense must inform defense" approach to prioritizing a list of the controls that would have the greatest impact in improving risk posture against real-world threats. A consortium of U.S. and international agencies quickly grew, and was joined by experts from private industry and around the globe. Ultimately, recommendations for what became the Critical Security Controls (the Controls) were coordinated through the SANS Institute. In 2013, the stewardship and sustainment of the Controls was transferred to the Council on CS (the Council), an independent, global non-profit entity committed to a secure and open Internet.

The Critical Security Controls focuses first on prioritizing security functions that are effective against the latest Advanced Targeted Threats, with a strong emphasis on "What Works" - security controls where products, processes, architectures and services are in use that have demonstrated real world effectiveness. Standardization and automation is another top priority, to gain operational efficiencies while also improving effectiveness. The actions defined by the Controls are demonstrably a subset of the comprehensive catalog defined by the NIST SP 800-53. The Controls do not attempt to replace the work of NIST, including the CS Framework developed in response to Executive Order 13636. The Controls instead prioritize and focus on a smaller number of actionable controls with high-payoff, aiming for a "must do first" philosophy. Since the Controls were derived from the most common attack patterns and were vetted across a very broad community of government and industry, with very strong consensus on the resulting set of controls, they serve as the basis for immediate high-value action.
SANS Institute’s “Top 20 Critical Security Controls” (Version 6) Follow the Hyperlinks to learn more about a particular security control

1. Inventory of Authorized and Unauthorized Devices
2. Inventory of Authorized and Unauthorized Software
3. Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers
4. Continuous Vulnerability Assessment and Remediation
5. Malware Defenses
6. Application Software Security
7. Wireless Access Control
8. Data Recovery Capability
9. Security Skills Assessment and Appropriate Training to Fill Gaps
10. Secure Configurations for Network Devices such as Firewalls, Routers, and Switches
11. Limitation and Control of Network Ports, Protocols, and Services
12. Controlled Use of Administrative Privileges
13. Boundary Defense
14. Maintenance, Monitoring, and Analysis of Audit Logs
15. Controlled Access Based on the Need to Know
16. Account Monitoring and Control
17. Data Protection
18. Incident Response and Management
19. Secure Network Engineering
20. Penetration Tests and Red Team Exercises
CONFIGURATION CHANGE MANAGEMENT PROCESS

The steps below show the process for a Configuration Change Management (CCM) that is approved at each step and shows the fields that must be documented on the CCM form. The form MUST be completed in the order listed below to ensure proper Change Management.

Requester completes the fields listed below:
Type of Device (Choice) -
Description (Multiple lines of text) -
System Name (Choice) -
Priority (Choice) -
Due Date (Date and Time) -
Comments (Multiple Lines of text) -
Assigned To (Person or Group) -

The LCPO assigns the request to an individual for research to determine the impact to the Network by completing the fields below:
Comments (Multiple lines of text) -
Issue Status (Choice) -
Assigned To (Person or Group) -

Network Administrator finishes Research of CCM impact to Network and completes the fields below:
Comments (Multiple lines of text) -
Research Man-hours (Number) -
Research Completed (Date and Time) -
Issue Status (Choice) -
Assigned To (Person or Group) -

The request for change is routed though the CCM review process as follows:
ADP Officer Approval (Choice) -
ISSM Approval (Choice) -
CSIO Approval (Choice) -
CCM Approval Date (Date and Time) -
Comments (Multiple lines of text) -
Issue Status (Choice) -
Assigned To (Person or Group) -
- Note - Depending on the impact may require higher authorization

Enclosure (14)
Upon completion of the CCM review, the CCM makes a recommendation to the Combat Systems Officer (CSO) and must complete the following fields:
- Comments (Multiple lines of text)
- Issue Status (Choice)
- Assigned To (Person or Group)

The CSO reviews the CCM recommendations. The CSO can approve, disapprove, defer the CCM for additional information, or forward to the Commanding Officer for approval. The fields below should be completed for approval:
- Comments (Multiple lines of text)
- Issue Status (Choice)
- Assigned To (Person or Group)

The Network Administrator will request an appropriate maintenance window and upon completion of the work fill-in the following fields:
- Physical Change Man-hours (Number)
- Physical Change Completed (Date and Time)
- Comments (Multiple lines of text)
- Issue Status (Choice)
- Assigned To (Person or Group)

The ISSM is responsible for updating the Network Drawings & Equipment List will document completion by completing the fields below:
- Network drawings & Equipment list Update Man-hours (Number)
- Network Drawings & Equipment List Updated (Date and Time)
- Comments (Multiple lines of text)
- Issue Status (Choice)
- Assigned To (Person or Group)
APPENDIX A
LIST OF REFERENCES

Compiled References can also be found at NAVIDFOR portal site, URL (o) by browsing: Public Documents □ References □ Commander’s CS Handbook Reference Library

Referenced in the text of this publication:

(a) Navy Cyber Power 2020, Office of the Deputy Chief of Naval Operations for Information Dominance (N2/N6)


(c) National Security Agency, Information Assurance Solutions Group. "Defense in Depth: A practical strategy for achieving Information Assurance in today’s highly networked environments."

(d) DoDI 8500.01, CS, dtd 14 March 2014

(e) OPNAVINST 5239.1C, Navy Information Assurance Program

(f) SECNAVINST 5239.3B, DON Chief Information Officer (CIO) Network Policy

(g) SECNAV M-5239.2, DON Information Assurance (IA) Workforce Management Manual

(h) SECNAV INST/MANUAL 5510.36 DON IS Program Manual

(i) NTD 07-09 (ALCOM 103/09, 231600Z JUN 09), Implementation Instructions and Restrictions on the Deployed DAA

(j) FLTCYBERCOM, Revised CSI Grading Guidance (U) message, DTG: 162020Z Jul 12

(k) DoDI 8500.2, Information Assurance Implementation, dtd 06 February 2003 (cancelled by DoDI 8500.01 but still referenced in Navy guidance)
(l) Chairman of the Joint Chiefs of Staff (CJCS) Manual 6510.01F, Cyber Incident Handling Program

(m) SECNAVINST 5239.19, DON Computer Network Incident Response and Reporting Requirements

(n) NTD 11-08 (ALCOM 156/08, 032052Z Nov 08), NCDOC Electronic Spillage Response

(o) DoDI 8510.01 RMF for DoD IT, March 12, 2014

(p) USCYBERCOM CTO 08-005 (23 Apr 08), Scanning and Remediation

(q) NAVNETWARCOM Communications Tasking Order (CTO) 11-16 (061955ZJul 11), SCCVI and VRAM Requirements

(r) NAVNETWARCOM (CTO) 11-16A (061431Z Sep 11), Secure configuration Compliance Validation Initiative and Vulnerability Remediation

(s) FLTCYBERCOM, FRAGO 01 to TASKORD 13-018 that Extended the Navy Implementation Deadline of ACAS to 15 Oct 2013 (U) message, DTG 281613Z Jan 14

(t) DISA Field Security Operations, CCRI Contributing Factors, revised 31 Jul 2013

(u) NAVNETWARCOM Computer Tasking Order (CTO) 08-05A (221515Z Jul 08), Standard Consent Banner and User Agreements

(v) USCYBERCOM Communications Tasking Order (CTO) 09-002 (15 May 09), Disabling Autorun

(w) FRAGO 12 to USCYBERCOM OPORDER 05-01 (Validation of DoD and IC Cross Domain Solutions) 26 Nov 08

(x) USCYBERCOM OPORD 12-1016, 21 August 2012, HBSS Deployment and Operations

(y) NAVNETWARCOM Communications Tasking Order (CTO) 12-10 (021800Z Aug 12), HBSS Deployment and Sustainment

(z) SCCVI eEye Digital Security Retina NETSEC Scanner User Guide v2.0 (Space and Naval Warfare Systems Center Pacific), revised 28 September 2012
(aa) USCYBERCOM Communications Tasking Order (CTO) 07-015 (11 Dec 07), PKI Phase II

(ab) NAVNETWARCOM Computer Tasking Order (CTO) 09-07 (091624Z Jul 09), PKI Implementation and Enforcement

(ac) NAVNETWARCOM Computer Tasking Order (CTO) 08-08 Change 4 (170135Z Nov 08), available via SIPRNET, URL (e)

(ad) SECNAV M-5510.30, DON Personnel Security Program

(ae) COMNAVIDFORINST 5239.3 (series), Cybersecurity Readiness Manual (CSRM)

Supporting references from which this publication was derived:

(af) NIST SP 800-128, Configuration Management Guide for IS

(ag) SECNAVINST 5520.3B, Criminal and Security Investigation and Related Activities within the Department of the Navy


(ai) DON DIACAP HANDBOOK V 1.0

(aj) CJCS Instruction 6510.01F, Information Assurance (IA) and Support to CND

(ak) DON CIO 221246Z AUG 07, DON CIO Goals

(al) Joint DoD Intelligence Information System/Cryptologic Sensitive Compartmented Information (SCI) Systems Security Standards Rev 4

(am) NTD 06-10 (ALCOM 137/10, 101721Z Sep 10), Password Requirements

(an) NAVNETWARCOM Computer Tasking Order (CTO) 08-11 (040150Z Dec 08), Implementation of INFOCON Level 3

(ao) NIST SP 800-34 Rev. 1, Contingency Planning Guide for IT Systems
(ap) DoD 8140.01, Cyber Security Workforce Management


(ar) OPNAV 5239/14 (REV 9/2011), SAAR-N

(as) DoDINST 8520.2, PKI and Public Key Enabling

(at) INSURVINST 4730.27, IS Material and Security Inspection

(au) OPNAVINST 5450.345, Mission, Functions, and Tasks of Commander, U.S. Fleet Cyber Command and Commander, U.S. Tenth Fleet

(av) FLTCYBERCOM, CS Certification & Accreditation Testing Guidance (U) message, DTG: 241233Z Jan 14

(aw) ICMC Student Guide (CIN: A-202-0041)

(ax) USCYBERCOM Communications Tasking Order (CTO) 08-008 (09 May 08), Policy on Use of Department of Defense (DoD) Standard Notice and Consent Banner and User Agreement

(ay) FLTCYBERCOM TASKORD 15-012, VRAM replacing OCRS for Navy Cyber Compliance Reporting

APPENDIX B
LIST OF UNIFORM RESOURCE LOCATORS (URLS)

(a) NAVIDFOR – CS Work Force UNCLAS portal

(b) DISA IA Support Environment (IASE)
http://iase.disa.mil/

(c) 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 INFOSEC site
https://infosec.navy.mil

(e) NCDOC site
UNCLAS: https://www.ncdoc.navymil
GENSER: https://www.ncdoc.navysmil.mil

(f) 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.navymil

(h) Enterprise Mission Assurance Support Service (eMASS) (Site/System Authority to Operate and DIACAP package status)
https://emass-navy.csd.disa.mil/

(i) Naval Network Warfare Command (NNWC) UNCLAS portal site

(j) DISA IASE site. http://iase.disa.mil

(k) VRAM site
UNCLAS: https://vram.spawar.navymil (NIPR VRAM 2.0) GENSER:
https://vram.spawar.navysmil.mil (SIPR VRAM 2.0)
(l) SPAWAR SAILOR 2.1 site
UNCLAS: https://sailor.nmci.navy.mil
GENSER: https://sailor.spawar.navy.smil.mil

(m) DISA VMS
UNCLAS: https://vms.disa.mil
GENSER: https://vms.disa.smil.mil

(n) USCYBERCOM site
UNCLAS: https://www.cybercom.mil
GENSER: https://www.cybercom.smil.mil

(o) NAVIDFOR - CSICP Stage II TAV portal site
https://usff.portal.navy.mil/sites/NAVIDFOR/training/CSICP/SitePages/Home.aspx

(p) FLTCYBERCOM - Office of Compliance and Assessments CSICP portal site

(q) TWMS
https://twms.navy.mil/

(r) FLTMPS
https://ntmpsweb.ncdc.navy.mil/ftmps/

(s) JPAS

(t) FLTCYBERCOM /C10F CIO Policy Direction portal

(u) FedVTe
https://fedvte.usalearning.gov/

(v) Cyber Inspection Scoping Notebook
https://usff.portal.navy.mil/sites/NAVIDFOR/training/CSICP/Lists/CSICPSTAG/IIIPREPARATION/AllItems.aspx
# APPENDIX C

## GLOSSARY - ABBREVIATIONS AND ACRONYMS

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ABM</td>
<td>Asset Baseline Module (component of Host Based Security System)</td>
</tr>
<tr>
<td>ACAS</td>
<td>Assured Compliance Assessment Solution</td>
</tr>
<tr>
<td>AO</td>
<td>Authorizing Official</td>
</tr>
<tr>
<td>ATO</td>
<td>Authorization to Operate</td>
</tr>
<tr>
<td>C&amp;A</td>
<td>Certification and Accreditation</td>
</tr>
<tr>
<td>CCB</td>
<td>Configuration Control Board</td>
</tr>
<tr>
<td>CCI</td>
<td>Control Correlation Identifier</td>
</tr>
<tr>
<td>CCRI</td>
<td>Command Cyber Readiness Inspection</td>
</tr>
<tr>
<td>CD</td>
<td>Cross-Domain</td>
</tr>
<tr>
<td>CDS</td>
<td>Cross-Domain Solution</td>
</tr>
<tr>
<td>CI</td>
<td>Counterintelligence</td>
</tr>
<tr>
<td>CIN</td>
<td>Course Identification Number</td>
</tr>
<tr>
<td>CIO</td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>CJCS</td>
<td>Chairman of the Joint Chiefs of Staff</td>
</tr>
<tr>
<td>CJCSI</td>
<td>Chairman of the Joint Chiefs of Staff Instruction</td>
</tr>
<tr>
<td>CND</td>
<td>Computer Network Defense</td>
</tr>
<tr>
<td>CNDSP</td>
<td>Computer Network Defense Service Provider</td>
</tr>
<tr>
<td>CNSS</td>
<td>Committee on National Security Systems</td>
</tr>
<tr>
<td>CNSSI</td>
<td>Committee on National Security Systems Instruction</td>
</tr>
<tr>
<td>CNSSP</td>
<td>Committee on National Security Systems Policy</td>
</tr>
<tr>
<td>CNTT</td>
<td>Computer Network Team Trainer</td>
</tr>
<tr>
<td>CO</td>
<td>Commanding Officer</td>
</tr>
<tr>
<td>COI</td>
<td>Course of Instruction (training), or Community of Interest (social, IT infrastructure)</td>
</tr>
<tr>
<td>COMNAVAIRFOR</td>
<td>Commander Naval Air Forces</td>
</tr>
<tr>
<td>COMNAVIDFOR</td>
<td>Commander Navy Information Dominance Forces</td>
</tr>
<tr>
<td>COMNAVSUBFOR</td>
<td>Commander Naval Submarine Forces</td>
</tr>
<tr>
<td>COMNAVSURFOR</td>
<td>Commander Naval Surface Forces COMPSEC</td>
</tr>
<tr>
<td>COMSEC</td>
<td>Communications Security COOP</td>
</tr>
<tr>
<td>CONOPS</td>
<td>Continuity of Operations CONOPS Concept of Operations</td>
</tr>
<tr>
<td>CS</td>
<td>Cybersecurity</td>
</tr>
<tr>
<td>CSI</td>
<td>Cybersecurity Inspection</td>
</tr>
<tr>
<td>CSICP</td>
<td>Cybersecurity Inspection and Certification Program</td>
</tr>
<tr>
<td>CSI-J</td>
<td>Cybersecurity Inspection-Joint CSI-N Cybersecurity Inspection-Navy</td>
</tr>
<tr>
<td>CSM</td>
<td>Command Security Manager</td>
</tr>
<tr>
<td>CSS</td>
<td>Central Security Service</td>
</tr>
<tr>
<td>CSWF</td>
<td>Cybersecurity Workforce</td>
</tr>
<tr>
<td>CSWIP</td>
<td>Cybersecurity Workforce Improvement Plan</td>
</tr>
<tr>
<td>CTO</td>
<td>Computer Tasking Order</td>
</tr>
</tbody>
</table>
FLO  Foreign Liaison Office
FLTCYBERCOM  Fleet Cyber Command
FLT MPS  Fleet Training Management Planning System
FN  Foreign National
FTP  File Transfer Protocol
GIG  Global Information Grid (discontinued term), now
      DoD Information Network, or DoDIN
GSA  General Services Administration
HBSS  Host Based Security System
HIPS  Host Intrusion Prevention System (component of
      Host Based Security System)
IA  Information Assurance (discontinued term), now
      Cybersecurity
IAM  Information Assurance Manager (discontinued term), now
      Information System Security Manager
IAO  Information Assurance Officer (discontinued term), now
      Information System Security Officer
IASE  Information Assurance Support Environment (URL (b))
IAT  Information Assurance Technical (discontinued term), now Privileged User
IAVA  Information Assurance Vulnerability Alert
IAVB  Information Assurance Vulnerability Bulletin IAVM
      Information Assurance Vulnerability Management IAVT
      Information Assurance Vulnerability Technical Notice
ICMC  Information and Communications Manager Course
      (CIN A-202-0041)
IMA  Intermediate Maintenance Activity
INFOCON  Information Condition
INFOSEC  Information Security
IR&R  Incident Response and Recovery
IS  Information System
ISA  Internet Security and Acceleration (web proxy used
      for Integrated Shipboard Network System)
ISEA  In-Service Engineering Activity
ISIC  Immediate Superior in Command
ISNS  Integrated Shipboard Network System
ISO  Information System Owner
ISSM  Information System Security Manager
ISSO  Information System Security Officer
IT  Information Technology
IT-21  Information Technology for the 21st Century
      (afloat/ashore networking concept)
JPAS  Joint Personnel Adjudication System (URL (s))
LAA  Limited Access Authorization
MA  McAfee Agent (component of Host Based Security System)
MAC  Mission Assurance Category
MIP  Maintenance Index Page (3M)
MS&A  Modeling, Simulation and Analysis
NBT  Navy Blue Team
NBTA  Navy Blue Team Assessment
NCDOC  Navy Cyber Defense Operations Command
NCTAMS  Navy Computer and Telecommunications Area Master Station
NCTS  Navy Computer and Telecommunications Station
NEC  Navy Enlisted Classification
NETSEC  Network Security
NIOC  Navy Information Operations Command
NIPRNet  Non-Classified Internet Protocol Router Network
NIST  National Institute of Standards and Technology
NSA  National Security Agency
NTD  Navy Telecommunications Directive
OCA  Office of Compliance and Assessment (Fleet Cyber Command)
OCRS  Online Compliance Reporting System
ODAA  Office of the Designated Accrediting Authority
O-FRP  Optimized Fleet Response Plan
OPSEC  Operational security
OPTAR  Operational Target (funding)
OPT  Operational Planning Team
OPLAN  Operational Planning
OT&E  Operational Test And Evaluation
PAO  Principal Authorizing Official
PEO C4I  Program Executive Office for Command, Control, Communications, Computers and Intelligence
PHYSEC  Physical Security
PII  Personally Identifiable Information
PIT  Platform Information Technology
PKI  Public Key Infrastructure
PM  Program Manager
POA&M  Plan of Action and Milestones
PoR  Program of Record
PRIVAC  Privileged Access (e.g. system administrator) RMF
Management Framework
SA  System Administrator
SAAR-N  System Access and Authorization Request-Navy
SAP  Special Access Program
SCAP  Security Content Automation Protocol
SCCVI  Secure Configuration Compliance Validation Initiative
SCI  Sensitive Compartmented Information
SECNAV  Secretary of the Navy
SF  Standard Form
SIPRNet  Secret Internet Protocol Router Network
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SLA</td>
<td>Service-Level Agreement</td>
</tr>
<tr>
<td>SOP</td>
<td>Standard Operating Procedure</td>
</tr>
<tr>
<td>SOVT</td>
<td>System Operability and Verification Testing</td>
</tr>
<tr>
<td>SP</td>
<td>Special Publication</td>
</tr>
<tr>
<td>SPAWAR</td>
<td>Space and Naval Warfare Systems Command</td>
</tr>
<tr>
<td>SPAWARSYSCEN</td>
<td>Space and Naval Warfare Systems Center STIG</td>
</tr>
<tr>
<td>T&amp;E</td>
<td>Test and Evaluation</td>
</tr>
<tr>
<td>TAV</td>
<td>Training and Assist Visit</td>
</tr>
<tr>
<td>TRANSEC</td>
<td>Transmission Security</td>
</tr>
<tr>
<td>TSCE</td>
<td>Total Ship Computing Environment</td>
</tr>
<tr>
<td>TSN</td>
<td>Trusted Systems And Networks</td>
</tr>
<tr>
<td>TYCOM</td>
<td>Type Commander</td>
</tr>
<tr>
<td>URL</td>
<td>Universal Resource Locator (internet hyperlink) USB</td>
</tr>
<tr>
<td>USFFC</td>
<td>United States Fleet Forces Command</td>
</tr>
<tr>
<td>USSTRATCOM</td>
<td>United States Strategic Command</td>
</tr>
<tr>
<td>VRAM</td>
<td>Vulnerability Remediation Asset Monitor (URL (k)) VSE</td>
</tr>
<tr>
<td>XO</td>
<td>Executive Officer</td>
</tr>
</tbody>
</table>

C-5