

OPNAV INSTRUCTION 5239.1D

From: Chief of Naval Operations

Subj: U.S. NAVY CYBERSECURITY PROGRAM

Ref: See enclosure (1)

Encl: (1) References (2) Risk Management Framework Taxonomy

1. Purpose

a. This instruction establishes policies, procedures, and assigns responsibilities for executing and maintaining the United States Navy's (USN) Cybersecurity Program and implements the provisions of references (a) through (aw).

b. Specifically included in this instruction is the USN policy and the responsibilities pertaining to reference (a), which replaces the Department of Defense (DoD) information assurance certification and accreditation process (DIACAP) with the risk management framework for DoD information technology (IT). This instruction is a complete revision and should be reviewed in its entirety.

- 2. Cancellation. OPNAVINST 5239.1C and NAVADMIN 081/12.
- 3. <u>Scope and Applicability</u>

a. This instruction is consistent with and supports references (b) and (c), and includes roles and responsibilities that enable the Office of the Chief of Naval Operations (OPNAV), the fleet, echelon 2 commands, systems commands (SYSCOM), type commands, program executive offices (PEO), and other development and acquisition activities to implement cybersecurity. It applies to all USN activities and organizations, as well as contractors and their sub-contractors, and contractor facilities (with appropriate contract provisions) that perform the functions in subparagraphs 3a(1) through 3a(4).

(1) Design, construct, operate, maintain, upgrade, procure, test, access, use, oversee, or manage Navy collateral and general service top secret and below USN networks and information systems (IS) used to receive, process, store, display, or transmit DoD classified or unclassified information. This may or may not comprise a National Security System and includes use in foreign military sales (FMS) programs (incorporation of cyber capabilities in FMS platforms will be in line with technology releasability policies for FMS customers). IT is the collective term that encompasses IS, platform IT or industrial control systems IT products, IT services, and any other IT asset. With regards to risk management framework and the rest of this instruction, there is no assessment and authorization process distinction between platform IT or industrial control systems and other IT.

(2) Process data or information regardless of classification and not limited to national security information as defined in reference (d).

(3) Operate systems on behalf of USN or own facilities or systems that process any information associated with USN contracts. Contractors processing classified information must also comply with reference (e). Contractors processing personally identifiable information must also comply with reference (f) and DoD Instruction 8582.01 of 6 June 2012.

(4) Operate systems, infrastructure, software, or platforms on behalf of USN or own facilities or systems that process any information associated with cloud service providers or cloud service offerings outlined in reference (g).

b. For the purposes of this instruction, the terms "fleet commanders" and "fleet" refer to operational forces inclusive of all warfighting domains, to include U.S. Fleet Forces Command (USFLTFORCOM), U.S. Pacific Fleet (COMPACFLT), and numbered fleet commands.

c. This policy will not alter or supersede the existing authorities and policies of the Director of National Intelligence and Deputy Chief of Naval Operations for Information Warfare (CNO (N2N6)), as the Navy head of the intelligence community (IC) element, regarding the protection of

sensitive compartmented information (SCI) as directed by references (h) and (i). Additionally, this policy will not alter or supersede the existing authorities and policies of the Director, Department of the Navy (DON) Special Access Program Central Office set forth in references (j), (k), and (l), Executive Order 12344, and section 7158 of Title 42, U.S. Code.

d. This policy does not alter or supersede the existing authorities of the Director, Naval Nuclear Propulsion Program (CNO NOON), who also serves as the Naval Sea Systems Command Deputy Commander for Nuclear Propulsion Program (NAVSEASYSCOM 08) and National Nuclear Security Administration Deputy Administrator for Naval Reactors, as set forth in sections 2401 and 2511 of Title 50, U.S. Code. The responsibilities detailed in subparagraph 8f align with and reinforce the existing responsibilities of CNO NOON for the supervision of all technical aspects of the Naval Nuclear Propulsion Program (NNPP), including oversight of program support in the area of cybersecurity of naval nuclear propulsion information (NNPI) and NNPP-related systems.

e. This policy is not to be interpreted as contradictory to the authority of operational commanders (e.g., carrier or expeditionary strike group commanders) and commanding officers regarding their responsibilities as outlined in the Navy Regulations. This instruction incorporates cybersecurity with their responsibilities to maintain readiness, organize forces and resources, develop training strategies and plans, act in self-defense of the unit, and immediately report departure from instructions.

f. This policy is intended to bridge the gap between DoD's replacement of the term information assurance (IA), as used in reference (m), with its successor cybersecurity. While applicable policies are under revision, the term cybersecurity as used in this policy will replace the term IA where applicable.

g. This instruction is aligned with and designed to be implemented harmoniously with the DON Cybersecurity Safety (CYBERSAFE) Program, reference (n). CYBERSAFE is intended primarily to identify and ensure sufficient protection and resiliency of mission critical IT in a contested environment, and does not conflict with the intent or execution of risk management framework. CYBERSAFE is not a substitute for risk management framework.

h. Federal, DoD, and DON policy take precedence over any conflicting requirements of this instruction. Implementing authorities should identify conflicting policy to DON Deputy Chief Information Officer (Navy) (DDCIO(N)) for resolution.

4. Background

a. Per reference (o), cybersecurity consists of the technical and managerial measures that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities. The USN risk management framework strategy includes disaster recovery and continuity of operations as operational, technical, and managerial measures.

b. Cybersecurity is a critical mission area of real world adversary active engagement and conflict. As such, it must be addressed as a peer mission area, along with the traditional USN missions in acquisition, modernization, maintenance, and operations.

c. Cybersecurity plays a critical role foundational to the conduct of naval operations. To position the Navy to fight and win with speed and agility in the increasingly connected and contested cyber domain, decisive, prioritized action is required to ensure robust, resilient, and sustainable cyber defenses.

d. The USN implementation of the risk management framework for DoD IT uses a hierarchical construct that recognizes the imperatives of ensuring cybersecurity as a fundamental component of mission capability. This construct:

(1) ensures cybersecurity is an integral part of the systems engineering process for all IT; and

(2) leverages mission areas technical authority (TA), domain-expertise and certification authority as specified by references (a), (c), and (p). USN implementation of the risk management framework is codified in enclosure (2) and is consistent with the DoD risk management framework Knowledge Service's process guide (https://rmfks.osd.mil/).

e. The security challenges confronting USN mission capability with respect to cybersecurity are intensifying as threats become increasingly sophisticated, persistent and diverse. As a result USN personnel, processes, and systems must also increase vigilance and capability to protect, detect, react, and restore full operations.

5. Objectives

a. Incorporate the basic goals of cybersecurity, as described in reference (o): Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wired communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation. This program further incorporates the necessity to defend and restore critical IT in a cyber-contested environment.

b. Establish hierarchical constructs for a USN cybersecurity chain of authority and responsibility, an risk management framework assessment and authorization process, and cybersecurity risk assessment process that aligns with the DoD and DON cybersecurity policies, Navy program budget, and TA and certification authority constructs. The term "certification authority" pertaining to reference (c) is the authority to certify that products meet established standards, and is different and distinct from the certification authority referenced in DIACAP. The DIACAP certifying authority provided risk assessments and authorization to operate (ATO) recommendations to the designated approval authority.

c. Delineate the specific categories of cybersecurity risk the USN is exposed to at all echelons, consistent with reference (o).

(1) <u>System Cybersecurity Risk</u>, or IS-Related Security <u>Risk</u>: Risk that arises through the loss of confidentiality, integrity, or availability of information or IT considering

impacts to organizational operations and assets, individuals, other organizations, and the Nation. A subset of information security risk.

(2) <u>Operational Cybersecurity Risk, or Information</u> <u>Security Risk</u>: The risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation due to the potential for unauthorized access, use, disclosure, disruption, modification, or destruction of information or IT.

(3) <u>Residual Cybersecurity Risk</u>: The amount of unmitigated risk that remains after respective security measures have been applied. In the context of risk management framework, this is often generically referred to as "risk."

d. As designated by DON Chief Information Officer (CIO), CNO (N2N6) in the role of DDCIO(N) is responsible for USN cybersecurity, directs the implementation of the USN's risk management framework strategy, and the USN cybersecurity risk management framework assessment and authorization processes, policies, and directives through the specifics set forth in this instruction, to:

(1) adopt a cybersecurity life-cycle risk management and continuous monitoring program, including an assessment of the remaining useful life of legacy systems compared with the cost of adopting current technologies and anticipation of future technologies; and

(2) achieve and maintain assessment and authorization of USN IT per reference (a).

6. Policy

a. The Navy will establish and use an integrated enterprise-wide decision structure for cybersecurity risk management (the risk management framework) that includes and integrates DoD mission areas pursuant to reference (p) and the governance process prescribed in this instruction.

b. Paragraph 8 below outlines organization-specific responsibilities for implementation of this policy.

c. The cybersecurity requirements for USN IT will be managed through the risk management framework for USN IT consistent with the principles established in references (a), (q), (r), and (s). Per enclosure (2), USN IT has begun the transition to the risk management framework following the tenets laid out in this instruction.

d. Enclosure (2) provides supplemental guidance and processes to be used by all authorizing officials (AO) for all Navy collateral and and general service top secret and below USN networks and IS in support of the USN implementation of risk management framework.

e. The Navy implementation of risk management framework will satisfy the statutory requirements of reference (d). DoD and Navy must meet or exceed the standards required by the Office of Management and Budget and the Secretary of Commerce, pursuant to reference (d).

f. At the start of the risk management framework process, USN IT must be categorized under reference (t), to implement a corresponding set of security controls from references (r) and (s). They should use assessment procedures from reference (u), and both DoD and DON specific assignment values, overlays, implementation guidance, and assessment procedures found on the DoD Knowledge Service at https://rmfks.osd.mil/. To ensure a consistent approach and implementation across the Navy enterprise, all applicable IT/Cybersecurity Technical Advisory Board (IT/CS TAB) standards must be followed. These requirements will provide a defendable enterprise, inheritance of controls, compensating measures, as well as translations from high level security controls to measureable and testable requirements specific to Navy environments. The IT/CS TAB supersedes the IT/Information Assurance Technical Authority Board in name only. A new charter will be released by Space and Naval Warfare Systems Command (SPAWARSYSCOM) to reflect this change.

g. Resources for implementing the risk management framework must be identified and allocated as part of the Navy Planning, Programming, Budgeting, and Execution process.

h. Each USN IT asset and DoD partnered system must have an AO (formerly known as designated approval authority) responsible

for authorizing the system's operation based on achieving and maintaining an acceptable risk posture to include any indications and warnings of possible exploit. This risk will be communicated to operational commanders and to Joint Force Headquarters Department of Defense Information Network (DoDIN). An ATO is not the same as a decision to operate. The decision to operate a USN IT asset or DoD partnered system in the operational environment is made by the operational commanders. The operational commander, based on the AO's risk determination and operational mission requirements, will decide whether or not to employ an asset, with or without authorization.

i. Cybersecurity reciprocity of DoD and other Federal agency and department IT authorizations is to be used to the maximum extent possible. AO refusals of reciprocity must be timely, documented, and reported to the DON Deputy Senior Information Security Officer (Navy) (DDSISO(N)) for review within 15 business days of submission.

j. Reciprocity is a mutual agreement among participating enterprises to accept each other's security assessments in order to reuse IT resources and to accept each other's assessed security posture in order to share capabilities. Specific to DoD and per the DoD CIO memorandum, "Cybersecurity Reciprocity" of 18 October 2016, cybersecurity reciprocity of assessment and authorization evidence developed by prior system authorization and deployments of sister DoD Components will be implemented to the maximum extent possible. Any such cybersecurity assessment, authorization, and testing conducted by another component must be evaluated before additional assessment or testing is USN components must conduct additional testing to undertaken. address unique conditions within the Navy environment, but they are neither authorized nor required to retest what another DoD Component has already tested. Program managers pursuing reciprocity must provide either the artifacts or system identification number to the cognizant security control assessor (SCA) and cognizant AO. Additionally, the program manager must provide the contact information of the system owner. The AO and SCA will then use the information provided to apply reciprocity to the maximum extent possible. Detailed reciprocity procedural guidance is contained in the the DDCIO(N) risk management framework process guide.

k. The risk management framework process will inform the acquisition processes for all USN IT, including requirements development, procurement and contractual documents (e.g. requests for proposals, statements of work, etc.), and both developmental test and evaluation and operational test and evaluation.

The USN risk management framework strategy will meet the 1. requirements of references (a) through (v) and the documents directly referenced in this instruction. This requires a continuous effort from the operational community in defining operational requirements. Per references (b) and (m), the primary USN parties responsible for ensuring implementation of cybersecurity requirements are the commanding officers of Navy organizations, program managers, SCAs, and the AOs. All USN IT, as defined in enclosure (2), must be safeguarded at all times to support a defense in depth (DiD) strategy. DiD is a strategy that integrates people, technology, and operational capabilities to establish variable barriers across multiple layers and dimensions of networks. Employing a DiD strategy leveraging multiple security countermeasures will help protect the integrity of USN platforms and IT assets in the enterprise.

m. Reference (a) requires owners of IS to ensure those systems are assessed and authorized as part of the development and acquisition process and throughout the system's operational lifecycle.

n. All USN IT are subject to the entire risk management framework process. The only distinction in the assessment and authorization routes will be whose authority the IT belongs to as defined in enclosure (2). Categorization will play an important role in tailoring the baseline of an IT asset's set of security controls to be implemented.

o. Inheritance is a situation in which IT receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the IT. These entities can be either internal or external to the organization where the IT resides. During the risk management framework process, system owners are expected to utilize inheritance in a risk-balanced, cost-effective manner. The PEO for Enterprise IS is responsible for providing control

inheritance to systems residing on the Navy/Marine Corps Intranet (NMCI) and the outside the continental USN enterprise network. The PEO for Command, Control, Communications, Computers and Intelligence is responsible for providing control inheritance to systems residing on consolidated afloat networks and enterprise services. Questions regarding inheritance for enterprise networks should be directed to the cyber security director for PEO for Enterprise IS and PEO for Command, Control, Communications, Computers and Intelligence.

7. <u>Future Cybersecurity Publications</u>. Future USN cybersecurity publications will detail roles and responsibilities for cybersecurity and cybersecurity-related matters not provided in this instruction. USN cybersecurity publications may also provide guidance when DON, Joint Staff, DoD, National Institute of Standards and Technology, Defense Information Systems Agency (DISA), and National Security Agency manuals and guides require additional detail or clarification for USN-unique systems or usage.

8. Responsibilities

a. <u>DoD Component Heads</u>. Reference (a) tasks the DoD Component Heads to:

(1) ensure that DoD IT under their authority is compliant with DoD and DON cybersecurity policies;

(2) ensure only IT with a current ATO, ATO with conditions, or interim authorization to test are operational; and

(3) ensure personnel engaged in or supporting risk management framework are appropriately trained and qualified per references (w) and (x).

b. CNO (N2N6)

(1) Serve as the accountable USN echelon 1 deputy chief of naval operations with roles and responsibilities for cybersecurity as defined by references (a), (b), (c), (y), and (z).

(2) As the DDCIO(N), following the provisions of reference (z), serve as the OPNAV cybersecurity requirements sponsor. Advocate for common cybersecurity requirements and ensure their inclusion as part of the mandatory system survivability key performance parameters in all new and emerging acquisition program Joint Capabilities Integration and Development System (JCIDS) documents.

(3) Coordinate with the IT/CS TAB to translate cybersecurity requirements into executable and measurable specifications that the IT/CS TAB can endorse, as defined by reference (aa).

(4) Ensure full coordination of USN risk management framework strategy execution with the Assistant Secretary of the Navy (ASN) for Research, Development, and Acquisition; Deputy ASN for Command, Control, Communications, Computers and Intelligence and Space; and DON CIO.

(5) Represent USN as the representative for all USN cybersecurity programs. Report Navy metrics to DoD and DON as required.

(6) Submit program objective memorandum requirements to support cybersecurity programs as delineated in the Navy Cyber Resiliency serial guidance. Coordinate with other resource sponsors to deliver holistic assessments and prioritized planning guidance to inform fiscal year execution and program objective memorandum actions.

(7) Plan, resource, and provide oversight for cybersecurity capabilities in advance of their projected deployment. This planning recognizes that cybersecurity capabilities require threat anticipation, specialized development, unique acquisition skills, and additional time for the risk management framework process. This includes advocating for requests for resources for IT under the sponsorship of other deputies chief of naval operations, when resiliency and sustainment of mission capability demands that systems must perform in a cyber-contested environment as described in the system survivability key performance parameters. All IT must be produced with cybersecurity capabilities commensurate to the

associated risk management framework findings. Product selection must follow existing analysis of alternatives and requirements validation processes.

(8) Approve and issue the USN's cybersecurity policy, systems management, and metrics documents; to include policy for the SCAs and AOs.

(9) Provide second endorsement and moderate deliberation between the cognizant AO and the DON CIO for any IT assessed by an SCA to be high or very high risk as part of the high risk escalation process. Recommend a risk decision to DON CIO that considers operational impact.

(10) Represent USN interests on various international, national, DoD, DON, and USN groups that develop cybersecurity policy.

(11) Serve as requirements sponsor for USN military and civilian cybersecurity workforce training requirements. Serve as resource sponsor for USN military information warfare community workforce.

(12) Identify USN IT critical assets and infrastructures following reference (y).

(13) Coordinate fleet requirements for the acquisition of communications security (COMSEC) material for DON.

(14) Draft and maintain the USN's cybersecurity instructions and manuals following references (a) and (y). This instruction will serve as a mandated cybersecurity standards reference for all other program architectural technical views (DoD Architecture Framework Standard Viewpoints 1 and 2) and USN cybersecurity standards input to the DoD IT Standards Registry.

(15) Ensure national security information is properly safeguarded from unauthorized disclosure by the classification of the information by the original classification authority.

(16) Serve as the USN cross domain support element per the DoD Instruction 8540.01 of 8 May 2015. Provide servicelevel process for identification and assessment of cross domain

interfaces, a process for integration and testing of existing cross domain solutions (CDS), and prioritization of CDS requirements.

(17) Sponsor, authorize, and budget for cybersecurity requirements assigned to CNO (N2N6).

(18) Serve as the USN risk executive function. Per reference (q), in this role CNO (N2N6) is responsible for ensuring:

(a) security risk-related considerations for individual IT, to include the authorization decisions, are viewed from a USN-wide perspective with regard to the overall strategic goals and objectives of the USN in carrying out its missions and business functions; and

(b) management of IT security risks is consistent across the USN, reflects USN cybersecurity risk tolerance, and is considered along with other organizational risks affecting mission and business success.

(19) Serve as USN representative to joint functional capability boards and Secretary of Defense investment review boards where those cyber efforts impact Navy missions.

(20) Oversee implementation of cybersecurity strategy and execution of policy across the entire scope of the Navy's cyber platform and lines of business to provide reasonable assurance of the Navy's combat, combat support, and support systems.

(21) Manage and oversee a DON CYBERSAFE program to provide maximum reasonable assurance of survivability and resiliency of critical warfighting systems, components, and processes.

(22) Using the USN's existing TA framework, ensure that common and rigorous technical standards and specifications underpin both the CYBERSAFE program and USN risk management framework.

(23) Monitor Navy's overall cyber risk posture by comprehensively reviewing various assessments, to include test and evaluation, inspections, and audits to identify trends and inform strategic adjustments if necessary.

(24) Coordinate and align processes with the other services and Joint Staff offices on implementation of higher level cybersecurity policy, directives, and initiatives.

(25) Establish and sustain the infrastructure to achieve the core cybersecurity functions that include: requirements definition and approval, cybersecurity strategy and compliance, cybersecurity resources oversight, and the CYBERSAFE program implementation and oversight.

(26) Coordinate with Naval Criminal Investigative Service (NCIS) to utilize law enforcement and counterintelligence capabilities throughout the DON cyberspace domain and network operations centers. These capabilities will provide rapid, coordinated law enforcement and counterintelligence pursuit, mitigation, and prosecution of the human elements associated with internal and external threats.

(27) Advocate for strengthened requirements for the protection of USN controlled unclassified information (CUI) while residing on or passing through contractor networks and systems.

(28) Per OPNAVINST 5510.165A, maintain an insider threat to cybersecurity program and portfolio as the designated Navy lead for insider threat to cyber-based aspects of the Navy Insider Threat Program.

(29) Establish a chain of authority and responsibility for the risk management framework process as per the following subparagraphs 8b(29)(a) through 8b(29)(h).

(a) Appoint functional authorizing officials (FAO) to collectively make risk decisions for the operation of all USN IT.

(b) Appoint OPNAV Special Program Division (OPNAV N9SP) as the AO and cybersecurity service provider for all Navy special access program (SAP) systems.

(c) Appoint Naval Intelligence Activity (NIA) CIO as the naval IC AO with direct liaison authority with respective IC CIOs and U.S. Fleet Cyber Command (FLTCYBERCOM) CIO in matters of naval IC IT security risk management.

(d) Appoint SCAs to assess risk for all classified and unclassified and general service top secret and below USN IT.

(e) Supervise the risk management framework AO council, in coordination with DON CIO; ensure enterprise awareness, review intra-mission decisions, domain decisions, make inter-mission decisions, domain decisions, review ongoing threats, trends and inspection results, and adjudicate differences amongst peer AOs. "Domain" in this paragraph refers to warfighting domain or mission areas, not classificationlevel.

(f) Approve and issue the USN's risk management framework cybersecurity policy, systems management, and metrics documents, to include USN risk management framework policies for the SCAs and AOs.

(g) Per references (b), (m), and (z), serve as the DDCIO(N) and submit all requests for continued operation of USN IT systems and circuits with aggregated high or very high system risk, as determined by the cognizant SCA, to DON CIO.

(h) Serve as DDSISO(N) and in this role:

<u>1</u>. coordinate and review USN reporting requirements as assigned by DoD CIO, DON CIO and applicable instructions and statutes; and

 $\underline{2}$. coordinate with the DON SAP Central Office for all SAP related cybersecurity.

c. Deputy Chief of Naval Operations for Fleet Readiness and Logistics (CNO (N4))

(1) Ensure cybersecurity implementation in USN facilities, industrial control systems, and logistics IS

including the implementation of USN risk management framework for assigned systems. Assess and resource these requirements for assigned assets.

(2) Plan, resource, and provide oversight for cybersecurity capabilities for assigned programs well in advance of the program's projected deployment. All IT must be produced with cybersecurity capabilities commensurate to the applicable risk management framework requirements.

d. <u>Deputy Chief of Naval Operations for Integration of</u> <u>Capabilities and Resources (CNO (N8))</u>. With CNO (N2N6) support, ensure USN cybersecurity and USN risk management framework requirements are incorporated during the deliberate requirements development process and implemented via the JCIDS process.

e. <u>Deputy Chief of Naval Operations for Warfare Systems</u> (CNO (N9))

(1) Resource validated cybersecurity requirements into warfare platforms and associated systems for safety, security, incident response, operations, manpower, and life cycle support.

(2) Program and resource requirements for assigned warfare systems programs commensurate with validated cybersecurity requirements during platform development and in advance of planned fleet operations. All IT must be produced with cybersecurity capabilities commensurate to the associated risk management framework findings.

f. CNO (NOON)

(1) Prescribe and enforce requirements relating to the protection of NNPI on all USN IT systems. These requirements are codified in reference (ab), its successor, and other formal policy issued by CNO (N00N).

(2) Serve as the sole AO and SCA for all NNPP IT systems that are physically part of, dedicated to, or essential in realtime to the operation of the propulsion plants of nuclearpowered ships.

(3) Provide review of and concurrence with all authorization decisions involving the processing of NNPI on USN IT systems not otherwise authorized by CNO (N00N).

(4) Establish formal agreements with FLTCYBERCOM Navy authorizing official (NAO) and other AOs, as appropriate, regarding reciprocity of authorization decisions, system interconnections between NNPP and non-NNPP IT systems, and procedures to execute the responsibilities listed.

g. <u>Director, DON SAP Central Office</u>. Following references (j), (k), and (ac), responsible for overseeing cybersecurity for SAP IT systems in the DON and is responsible for developing and implementing policies and procedures as it relates to cybersecurity for SAP IT systems in the DON.

h. FLTCYBERCOM

(1) Per references (ac) and (ad), serve as the operational authority for Navy networks, cryptology, signal intelligence, information operations, cyber, counterintelligence reporting and space to carry out mission, function and tasks.

(2) Ensure all operational cybersecurity requirements are properly implemented and managed for all classified and unclassified and general service top secret and below USN IT.

(3) Produce cyber risk assessments based on threat intelligence and vulnerability assessments, under their AO authority, and disseminate risk assessments to the USN operational commands, SYSCOMs, type commands, and report back to the Joint Force Headquarters DoDIN on the status of USN risk in relation to security of nationwide networks. Identify the impact of assessed risk and, when possible, mitigation following risk management framework and CYBERSAFE standards.

(4) Ensure metric data from Naval Network Warfare Command, Navy Information Command Norfolk, and Navy Cyber Defense Operations Command is collected to support DDCIO(N) and NAO. FLTCYBERCOM will direct operational subordinate commands to provide additional support to the AO Council as required. (5) Issue tasking orders as required to maneuver networks as necessary to respond to incidents; and support higher echelon tasking and policy issuance.

(6) Provide cybersecurity operational requirements to CNO (N2N6) annually for consolidation, prioritization, and final approval of a single set of Navy cybersecurity requirement priorities.

(7) Serve as the NAO for all classified and unclassified and general service top secret and below USN IT assets that are not under the cognizance of an FAO. The NAO will execute the functions outlined in enclosure (2). NAO signature authority will not be delegated below the O-6/GS-15 level due to the enterprise scope of their cognizance. These delegations must be appointed and maintained by Commander, FLTCYBERCOM with a copy provided to CNO (N2N6).

(8) As the Navy's Service cryptologic component, coordinate cybersecurity and cybersecurity-related program activities with the Director of National Security Agency staff. This includes, but is not limited to, managing and implementing cybersecurity actions such as information assurance vulnerability management (IAVM) processes for information operations and signal intelligence systems on the Navy's portion of networks under the jurisdiction of the Director of National Security Agency.

(9) Oversee and direct operation of USN IS networks including monitoring and restoration actions as defined by reference (ac). Actions may include performing Web risk assessment and analysis to determine vulnerabilities and mitigation strategies on all USN networks. Coordinate and direct appropriate actions to ensure that USN public-facing and non-public-facing Web pages comply with prescribed DoD, DON, and USN guidance.

(10) Coordinate defensive cyber operations (DCO) training to fleet units as requested by fleet commanders on an annual basis.

(11) Coordinate carrier strike group and expeditionary strike group computer network vulnerability analysis training

and testing. Establish memoranda of agreement with fleet commanders for this training. Provide metrics data to CNO (N2N6) that measures the cybersecurity readiness for platforms both before and after receiving computer network vulnerability analysis support.

(12) Manage the USN's IAVM program per reference (ae) and act as the USN's reporting agent for IAVM processes. Act as USN's reporting agent for computer tasking order processes.

(13) Serve as USN lead for ports, protocols, and services management to include Domain Name System.

(14) Coordinate with Commander, Operational Test and Evaluation Force (COMOPTEVFOR), USN commands, joint testing agencies, DISA, and other DoD and national organization to provide the required operational criteria to which personnel, tools, assets and capabilities must adhere, in order to maintain confidentiality, integrity, and availability when conducting operational actions in and through Navy cyberspace.

(15) Serve as one of the testing agents with COMOPTEVFOR as part of risk analysis and mitigation for new equipment and networks per the role specified in references (af) and (ag) in support of reference (ah) and all applicable director, operational test and evaluation guidance. This testing agent role is different than an risk management framework SCA role.

(16) Coordinate with operational subordinates to conduct penetration tests and vulnerability analysis during military exercises for Navy assigned systems and interfaces. Ensure tests do not expose hardware and software to risk of physical damage or logical corruption. This activity includes validating security compliance, DISA standards implementation, cybersecurity vulnerability management compliance, and the overall system cybersecurity posture.

(17) Per reference (ac), provide oversight and serve as lead for executing the cybersecurity inspection and certification program.

(18) Coordinate, monitor and oversee the defense of Navy computer networks and systems and execute DCO mission as per the following subparagraphs 8h(18)(a) through 8h(18)(p).

(a) Serve as the Navy's tier 2 cybersecurity service provider as per references (ae) and (ai), cybersecurity and support to computer network defense (CND).

(b) Determine when systems are under strategic computer network attack, contain damage, restore functionality, and provide feedback from forensic studies to the user community.

(c) Execute all actions required to protect, monitor, analyze, detect, react, and restore from unauthorized activity within Navy IS and computer networks.

(d) Coordinate USN efforts with other government and commercial activities to identify, assess, contain, and counter the impact of computer incidents on national security communications and IS, and to remediate or eliminate identified vulnerabilities.

(e) Develop requirements for and maintain an infrastructure that has the capacity and capability to maintain raw data required for forensics and trend analysis.

(f) Make information operations condition and cyber condition recommendations and report the Navy information operations condition and cyber condition status.

(g) Coordinate with other service and national level organizations and agencies to share information concerning vulnerabilities, threats, countermeasures and Navy computer network security incidents.

(h) Develop and implement contingency plans, tactics, techniques, and procedures to defend Navy computer networks. Operate a 24-hour per day, 7 days per week computer incident response team to centrally coordinate actions involving computer network security incidents and vulnerabilities, which threaten Navy computer networks worldwide.

(i) Monitor the current cybersecurity readiness of USN computer networks and maintain a global DCO user-defined operational picture for situational awareness.

(j) Oversee and conduct the cybersecurity vulnerability analysis and assessment activities for operational naval forces.

(k) Resource, train, and coordinate deployable flyaway support as required in response to USN network security incidents.

(1) Participate in joint and USN training exercises and refine DCO tactics, techniques, and procedures.

(m) Provide timely advisories for newly identified cybersecurity vulnerabilities.

(n) Provide the IC with priority intelligence requirements for collection and indications requirements for potential attacks against USN computers and networks.

(o) Leverage external assessments as necessary in support of DCO. Analyze external assessment exercise results and incorporate lessons learned into Navy CND service provider directives and guidance to subscribers for vulnerability mitigation and receive external assessments, after action reports, and confirmation of command implementation of required actions.

(p) Maintain electronic spillage center to ensure all aspects of negligent discharge of classified information (NDCI) on USN networks are properly addressed as per reference (ah).

i. <u>Commander, USFLTFORCOM, and Commander, COMPACFLT</u>. The echelon 2 supported commanders for implementation of fleet cybersecurity through the operation and maintenance of assigned operational units, facilities, and IT in their respective areas of responsibility (AOR). Responsible for the safe, secure, reliable and effective technical operation, maintenance, and cybersecurity of fielded platforms. Fleet commanders define requirements for various platforms to permit fighting in a contested cyber environment.

j. <u>Commander</u>, <u>USFLTFORCOM</u>. In conjunction with its subordinate commands, Navy Information Forces and Naval Communications Security Material System, USFLTFORCOM will:

(1) execute duties as information forces type commander following the Commander, USFLTFORCOM Instruction 5450.10A;

(2) maintain the central office of record; ensuring the proper storage, distribution, inventory, accounting, and overall safeguarding of COMSEC materials for the USN, Marine Corps, Coast Guard, Military Sealift Command, and Joint and Allied commands, as required;

(3) control, warehouse, and distribute cryptographic equipment, ancillaries, and associated keying material for the USN;

(4) write safeguarding and accounting instructions for Navy COMSEC material, and review, issue, publish, and distribute guidance necessary to ensure National level (e.g., National Security Agency) policies are followed and enforced throughout the lifecycle including disposal;

(5) serve as the Navy's high assurance public key infrastructure (PKI) certificate approving authority as described in reference (aj);

(6) serve as a Navy registration authority for medium
assurance (class 3) PKI;

(7) per reference (ak), serve as the DON COMSEC incident monitoring activity;

(8) per reference (ak), manage the DON COMSEC Inspection Program and establish standards for COMSEC inspectors and inspections;

(9) resolve COMSEC related technical queries and conflicts with members of CNO (N2N6) and national COMSEC community, plan for phased obsolescence, declassification, removal of COMSEC accounts and disposal of retiring COMSEC equipment; and

(10) per reference (ak), manage the DON COMSEC Training Program, and provide worldwide COMSEC advice and assistance to customers.

k. <u>Commander, Navy Installations Command (CNIC)</u>. The echelon 2 support to CNO (N4), CNO (N9), USFLTFORCOM, COMPACFLT, and Director, Strategic Systems Programs (SSP) for base operations support for facilities, facility sustainment, infrastructure sustainment, and military construction. CNIC will support OPNAV in the definition of USN risk management framework requirements and ensure cybersecurity and USN risk management framework are implemented in assigned AOR.

1. <u>Naval SYSCOMs</u>. Naval Air Systems Command (NAVAIRSYSCOM), Naval Facilities Engineering Command (NAVFACENGCOM), Naval Sea Systems Command (NAVSEASYSCOM), Naval Supply Systems Command (NAVSUPSYSCOM), and SPAWARSYSCOM are referred to collectively as "naval systems commands." SYSCOMs, along with SSP, are the echelon 2 supporting offices responsible for design, modification, upgrade, and maintenance of USN IT as applicable for their assigned AORs defined by reference (c) and this instruction. SYSCOM commanders' responsibilities include serving as TA and operational safety and assurance and system certification authorities as per reference (c).

(1) Direct, in coordination with the applicable resource sponsors, technical assessments including standards compliance consistency during design and development of all IT within their respective AORs to determine the possibility of cyber vulnerabilities. In the event vulnerabilities are discovered, direct the implementation of appropriate risk mitigations to protect against, detect, analyze, report, respond to, and recover from a cyber-incident to ensure system survivability and mission capability.

(2) Establish and implement standard cybersecurity and USN risk management framework requirements translated into procedures for the maintenance, use, sustainment, recomposition, and logistics support of systems and components under their jurisdiction.

(3) Design USN IT systems with the necessary components to ensure the safety and mission capability of the crew, the systems, and the platforms assigned.

(4) Develop and implement contingency plans, tactics, techniques, and procedures to defend all USN IT under their jurisdiction.

(5) Provide security engineering services for protection of critical assets and telecommunications infrastructures.

(6) Provide cybersecurity acquisition support to CNO (N2N6) (including CNO (N9) and CNO (N4) funded), FLTCYBERCOM, other SYSCOMs, and the Enterprise-Wide Solutions Steering Group on all cybersecurity acquisition program issues for assigned programs as a part of the USN enterprise risk management program.

(7) Implement standards, tools, and processes that SPAWARSYSCOM, as the cybersecurity TA, publish for a consistent cybersecurity assessment process for IT and networks via the IT/CS TAB. SYSCOMs will develop and implement installation assessments and system certifications for deployment processes based on these standards within their AOR per reference (c).

(8) Implement CYBERSAFE criteria following Secretary of the Navy (SECNAV) and OPNAV CYBERSAFE policies and manuals and requirements as part of the systems engineering processes at the systems, systems of systems, enclave, or platform IT or industrial control systems, and the platform integration levels of the platform architectures.

(9) NAVAIRSYSCOM, NAVFACENGCOM, NAVSEASYSCOM, SPAWARSYSCOM, and SSP will serve as FAOs for IT that meet the criteria of enclosure (2) and are in their respective AOR per reference (c). AO responsibilities are outlined in enclosure (2), USN risk management framework taxonomy. FAO signature authority will not be delegated below the flag officer (FO) or senior executive service (SES) level.

(10) SPAWARSYSCOM will recommend an FO or SES to serve as the USN SCA. The SCA will be jointly warranted with SPAWARSYSCOM as the cybersecurity TA and appointed by CNO (N2N6). SCA signature authority may not be delegated below the O-6/GS-15 level due to the enterprise scope of their cognizance. These delegations must be appointed and maintained by Commander, SPAWARSYSCOM, with a copy provided to CNO (N2N6). SCA responsibilities are outlined in enclosure (2).

(11) NAVAIRSYSCOM, NAVFACENGCOM, NAVSEASYSCOM, SPAWARSYSCOM, and SSP will recommend an FO or SES to serve as functional security control assessor (FSCA) for their respective AORs. FSCAs will be jointly warranted with SPAWARSYSCOM as the cybersecurity TA and appointed by CNO (N2N6). FSCA signature authority may not be delegated below the FO and SES level. FSCA responsibilities are outlined in enclosure (2).

(12) To enable centralized cybersecurity requirements, FAOs will annually provide cybersecurity operational requirements to CNO (N2N6) for consolidation and prioritization via the AO Council and final approval of a single set of Navy cybersecurity requirement priorities for CNO (N2N6) approval.

(13) As part of the SYSCOM platform (e.g., facility, aircraft, ship) certification process intrinsic to their certification responsibilities as defined by reference (c) for individual platforms, the SYSCOM commander will ensure a platform or enclave cybersecurity risk assessment is performed and maintained. These assessments will incorporate stakeholder inputs and aggregate cybersecurity risk for the platform. As an example, ship cybersecurity risk assessments will be conducted across enclaves and in collaboration with FLTCYBERCOM and the responsible cybersecurity TA representatives. This analysis will provide the cybersecurity readiness of the platform in a manner similar to the other platform readiness parameters currently reported by each platform. The cybersecurity readiness of the fleet can then be assessed by combining the platform cybersecurity risk assessments. The fleet cybersecurity readiness will then be combined with the Navy enterprise IS cybersecurity readiness posture and this Navywide cybersecurity readiness status can then be reported to the CNO by CNO (N2N6). This approach leverages both existing material and training readiness processes used across the Navy and the existing program, budget, technical, and certification authorities.

m. <u>PEOs, SYSCOMs, and SSP</u>. As appropriate, responsible for all aspects of life-cycle management of their assigned programs. Roles and responsibilities described in this paragraph below are not intended to assign, modify or reallocate roles and responsibilities as described in reference (c). This section provides additional detail, made necessary by changing and additional cybersecurity processes and programs such as risk management framework and CYBERSAFE respectively. As per reference (ag) and following reference (al), PEOs are responsible for planning and execution of in-service support,

and are responsible to the ASN for Research, Development and Acquisition for acquisition-related matters. In order to satisfy DoD cybersecurity guidelines outlined in reference (a) and to operate systems on DoD networks it is necessary that all programs under PEOs, SYSCOMs, and SSP perform the responsibilities in subparagraphs 8m(1) through 8m(13).

(1) In coordination with program managers, implement cybersecurity as an intrinsic element of their programs as prescribed by references (c), (am) (an), and (ao) and other applicable references across the life cycle of the platforms, IT and networks under their jurisdiction. This includes not only initial delivery but also maintenance and modernization needed to keep pace with commercial-off-the-shelf obsolescence and the evolution of the threats and their associated internal, external and supply chain vectors. Included in these responsibilities are the approved technical and operational procedures that address assessment and authorization and continuous monitoring for all IT, whether connected or standalone, and system material (hardware and software), operational, casualty, and maintenance control procedures needed for each system to ensure cybersecurity implementation and effectiveness.

(2) Ensure cybersecurity is a key element of program protection planning activities that manage risks to advance technology. Ensure that contracts and other agreements include specific requirements to provide for the safeguarding of CUI related to these systems while residing on contractor networks and systems per references (ao) and (ap).

(3) Ensure that new acquisition programs with JCIDS governing documents include the mandatory system survivability key performance parameters intended to provide survival and operation in a cyber-contested environment or after exposure to cyber threats. PEOs will implement standards and specifications endorsed by the IT/CS TAB and issued by the cybersecurity TA. PEOs are adjunct members of the Cybersecurity Executive Committee as established in the executive committee's charter, and members of the advisory board.

(4) Streamline the acquisition and management of cybersecurity solutions and services and align the development and acquisition of enterprise DoDIN solutions and capabilities with IT/CS TAB specifications, standards and guidance.

(5) Ensure PEO assigned programs are compliant with all applicable Federal Information Security Modernization Act reporting and cybersecurity requirements throughout the programs' lifecycle.

(6) Utilize information security systems engineers for required risk management framework tasks and to ensure adherence to appropriate technical standards, tools, and processes as approved by the cybersecurity TA.

(7) Provide input, review, and recommended updates to cybersecurity publications.

(8) Support all efforts to protect all USN IT under their jurisdiction.

(9) Provide assistance to Naval Education and Training Command on standards and training content associated with systems the PEOs acquire.

(10) Ensure cybersecurity products acquired comply with references (c) and (y), as implemented through the National Information Assurance Partnership, Common Criteria Evaluation and Validation Scheme, and acquisition of allied products validated under the International Organization for Standardization 15408, Common Criteria Program, and other applicable criteria.

(11) Execute and manage assigned Navy cybersecurity acquisition programs and projects, including associated research and development, and full life-cycle systems support.

(12) Ensure that all IT has a qualified and active information systems security manager (ISSM) and subordinate IS security officer as per reference (a). The program ISSM reports directly to the program manager on all matters involving cybersecurity with the acquisition program.

(13) Ensure that all standalone USN IT completes the risk management framework process as per AO direction and reference (a).

n. <u>PEO for Command, Control, Communications, Computers and</u> <u>Intelligence</u>. PEO Command, Control, Communications, Computers and Intelligence is the Navy cybersecurity acquisition program manager and serves as the acquisition lead on joint and coalition interoperability of cybersecurity capabilities. As such, the PEO for Command, Control, Communications, Computers and Intelligence implements and executes the following cybersecurity and cybersecurity-related products, programs, and services for assigned programs: cryptographic systems, CND, DCO, cyber defense situational awareness, continuous monitoring, secure voice, secure communications interoperability protocol interworking function, CDS, electronic key management system, key management infrastructure, PKI, and insider threat.

o. Commander, SPAWARSYSCOM

(1) Serve as the Navy's cybersecurity TA.

(2) Execute TA, which is the authority, responsibility, and accountability to establish, monitor, and approve technical standards, tools, and processes in conformance to higher authority policy, requirements, architectures, and standards, following references (c) and (aq).

(3) Serve as technical support agent to the CNO (N2N6) representative on the DoD CIO Enterprise-Wide Solutions Steering Group.

(4) Provide technical and non-technical system security evaluations and recommendations to Navy systems and networks as assigned.

(5) Provide cybersecurity system security engineering and other technical expertise to supporting SYSCOMs, PEOs, and other Navy development, acquisition, and operational activities for all Service, joint, and coalition programs as requested by the supported activities.

(6) Operate the Navy's Emanations Security Program to include providing certified telecommunications electronics material protected from emanating spurious transmissions TA.

(7) Warrant cybersecurity technical warrant holders and technical area experts within the other SYSCOMs as required.

(8) Jointly warrant, with the applicable SYSCOM, nominees for the SCAs. SPAWARSYSCOM will issue the cybersecurity warrant and the applicable SYSCOM will issue the technical warrant. These warrants are to be required in order to execute the duties of an SCA.

(9) Support USN's cybersecurity research and development activities.

(10) Issue proficiency standards and expectations for FSCAs and Navy qualified validators in coordination with the IT/CS TAB.

(11) Serve as the USN SCA for all business IS; command, control, communications, computers and intelligence IS; transport IS; and other systems as assigned by DDCIO(N) and execute duties as described in enclosure (2).

(12) Operate the Navy CDS Office in the capacity per the following subparagraphs 8o(12)(a) through 8o(12)(e).

(a) Serve as the USN office responsible for the recommendation to the system owner of a solution using either: a cross domain enterprise solution, one that is Unified Cross Domain Services Management Office compliant, or employing Navy unique cross domain technologies.

(b) Manage connection approval process activities for cross domain connections, to include ensuring that annual review of security controls are completed for all CDSs.

(c) Maintain USN cross domain support element records in the DoD cross domain database Secret Internet Protocol Router Network (SIPRNet) Global Information Grid Interconnection Approval Process System. Actively maintain CDS specific information in the DoD cross domain database to include device configuration, instantiation location on the networks, and site and system point of contact information. (d) Provide technical recommendations on cross domain interfaces to the NAO or FAO, as applicable, and USN cross domain support element.

(e) Serve as the USN's representative on the Cross Domain Technical Advisory Board.

IT/CS TAB. The IT/CS TAB was established by p. SPAWARSYSCOM under the Systems Engineering Stakeholder's Group and will support CNO (N2N6), define requirements and priorities to develop, approve, and distribute cybersecurity specifications and standards needed to define material (hardware-software) and controls needed to implement cybersecurity. The IT/CS TAB is expressly a cross-SYSCOM collaborative and integrated approach to ensure balanced application of standards and specifications, and the implementation of affordable solutions. The IT/CS TAB standards will ensure cybersecurity implementation is executable and measurable. The IT/CS TAB serves as the technical arm of CYBERSAFE, developing CYBERSAFE standards, processes, and tools, and resolving CYBERSAFE technical issues between SYSCOMs. The membership and roles and responsibilities of the IT/CS TAB are defined by reference (aa). Reference (aa) is subject to review and updates more frequently than this instruction and is therefore referenced instead of included in this instruction.

q. Commander, Naval Education and Training Command

(1) Develop Navy schoolhouse cybersecurity training and education.

(2) Ensure cybersecurity training is incorporated into all pertinent USN training and appropriate formal schools.

r. <u>NIA</u>. In conjunction with its subordinate command, Office of Naval Intelligence, NIA is responsible for the duties in subparagraphs 8r(1) through 8r(12).

(1) Serve as the naval IC authoritative senior cybersecurity leadership that represents CNO (N2N6) on all cybersecurity related IC working groups.

(2) Execute naval IC SCI IT systems security risk management and authorization authorities, and provide oversight

and guidance to support naval IC SCI cybersecurity program activities. Act as SCA and AO for all naval IC SCI cybersecurity program activities.

(3) Develop, de-conflict, and publish all Navy noncryptologic SCI cybersecurity program guidance, to ensure support of, and consistency with the Office of the Director of National Intelligence IC Enterprise Services, Defense Intelligence Agency, DoD Intelligence Information Service, DON enterprise, and IC directives, policies and guidance.

(4) Provide oversight, collection, validation and synchronization of Naval IC Federal Information Security Modernization Act reporting.

(5) Coordinate with USN cybersecurity stakeholders and IC CIO for Navy IC element CND concept of operations as appropriate.

(6) Coordinate with the naval IC cognizant security authority for administrative, personnel and physical security on appropriate protection of SCI.

(7) Provide all-source, fused intelligence support for USN. Production will be accomplished in coordination with the NCIS.

(8) Assist CNO (N2N6), FLTCYBERCOM, PEOS, SYSCOMs and the IT/CS TAB in the risk management process by gathering relevant threat information to assist in defining system security requirements.

(9) Provide all-source cyber collection and analysis, fused intelligence support to FLTCYBERCOM, numbered fleet commanders, strike group commanders, task force commanders, and the SYSCOMs as needed to support their cybersecurity activities. Production will be accomplished in coordination with the NCIS.

(10) Deliver in-depth trend analysis for indications and warnings of computer attacks and exploitation of National or Navy networks. Production will be accomplished in coordination with the NCIS.

(11) To enable centralized cybersecurity requirements, NIA will annually provide cybersecurity operational requirements to CNO (N2N6) for consolidation and prioritization via the AO Council and final approval of a single set of Navy cybersecurity requirement priorities for CNO (N2N6).

(12) Serve as the Navy lead for the development and implementation of plans and programs designed to coordinate and manage the counterintelligence, cybersecurity, anomaly detection, personal security, and continuous evaluation mission areas of the Navy Insider Threat Program, per reference (ar).

s. Commanders of Navy Echelon 2 Organizations

(1) Appoint in writing a CIO.

(2) Ensure through the CIO compliance with all cybersecurity directives and policies, and ensure the systems' development life cycle incorporates cybersecurity and interoperability.

(3) Comply with cyberspace IT and cybersecurity workforce qualification and continuous education training requirements as stated in reference (as).

(4) Request vulnerability assessment assistance from Navy Information Command Blue Team operations to validate cybersecurity controls and practices.

(5) Validate the implementation of cybersecurity policy through automated tools and formalized cybersecurity checklists (assessments and inspections).

(6) Ensure all IT systems and assets within their purview are fully authorized by the appropriate AO prior to operation or connection, and be prepared to cease operation of all systems and assets if cybersecurity authorizations are revoked or expired.

(7) Delegate an echelon 2 package submitting officer who is responsible for ensuring that assessment and authorization packages are submitted following timelines and guidance established by DDCIO(N).

(8) Ensure IS network managers, command security managers, and ISSMs understand their responsibilities and address all aspects of NDCI and electronic spillage on USN networks and work with the Navy electronic spillage center to expeditiously resolve all processes and procedures associated with electronic spillage.

(9) Ensure local processes and procedures for reporting and responding to an NDCI are following reference (v).

(10) Ensure all contract line item numbers associated with the cleanup of NDCI on the NMCI Enterprise are ordered and processed under reference (at).

(11) Ensure all command-level security managers, ISSMs, and network users within their AOR understand their responsibility to protect classified data and controlled unclassified data (e.g., for official use only and personally identifiable information) and immediately report a suspected NDCI to their command security manager, ISSM, and immediate chain of command.

(12) Comply with all rules and policies to securely operate all CDSs under their purview. Document and submit any new or changing CDS requirements as soon as known to the Navy CDS Office.

(13) Validate the operational requirements for new requests for cross domain capabilities and verify the requested capability does not already exist. Submit a request to the cognizant AO requesting AO and DDCIO(N) endorsement of the request to enter the CDS connection approval process.

(14) Annually verify that the operational requirement still exists for cross domain connections to the appropriate AO.

(15) Provide direct support of the CDS connection approval process and annual revalidation requirements for cross domain devices and hosting command communications service designator).

(16) Actively monitor and support SIPRNet connection approval process and CDS connection approval process activities. Coordinate with the Navy CDS Office to ensure accurate command

communications service designator and CDS information are contained in the SIPRNet Global Information Grid IA Portfolio.

(17) Actively monitor and support the modernization of the CDS within each respective AOR and assist in the submission of the cross domain appendix for each AOR.

(18) Ensure all personnel performing cybersecurity functions receive initial basic and system specific training, obtain required certification as required in reference (as), and complete annual recurring, refresher, or follow-on training per references (w) and (x).

(19) Ensure cybersecurity awareness indoctrination training is tailored to specific site requirements. Ensure users complete the DoD authorized annual cybersecurity refresher training and retain documentation. Ensure each user also completes the OPNAV 5239/14 System Authorization Access Request-Navy form and that the command retains this form for the duration of the user's access.

(20) Ensure awareness and reporting training for counterintelligence and insider threat is completed per reference (au) and reporting occurs following reference (ad).

(21) Ensure any suspicion or confirmation of a computer intrusion incident is reported per reference (ah) and joint policy including reference (ae). Reports include the operational chain of command for situational awareness as required by reference (ah).

(22) Report all actual or suspected felony criminal activities and cyber-related activities associated with espionage, terrorism, sabotage, unauthorized access, intrusion, denial of service, viruses, or malicious code to NCIS and FLTCYBERCOM.

(23) When a unit is deployed make mission-based operational decisions in coordination with the appropriate AO, regarding authorizing the use of, or changes to, IT assets. The appropriate AO must be notified of changes to the configuration of any IT asset as soon as practicable. The process to request an ATO with the new configuration must be implemented or the IT asset must be returned to the approved configuration.

(24) Ensure assessment and authorization team members are assigned following reference (a).

(25) Ensure that personnel develop and exercise continuity of operations and contingency plans for denial or disruption in service due to cyber incidents.

9. Records Management

a. Records created as a result of this instruction, regardless of media and format, must be maintained and dispositioned for the standard subject identification codes (SSIC) 1000, 2000, and 4000 through 13000 series per the records disposition schedules located on the Department of the Navy/Assistant for Administration (DON/AA), Directives and Records Management Division (DRMD) portal page at https://portal.secnav.navy.mil/orgs/DUSNM/DONAA/DRM/Records-and-Information-Management/Approved%20Record%20Schedules/Forms/AllItems.aspx. For SSIC 3000 series dispositions, please refer to part III, chapter 3, of SECNAV Manual 5210.1 of January 2012.

b. For questions concerning the management of records related to this instruction or the records disposition schedules, please contact your local records manager or the DON/AA DRMD program office.

10. <u>Review and Effective Date</u>. Per OPNAVINST 5215.17A, CNO (N2N6) will review this instruction annually on the anniversary of its effective date to ensure applicability, currency, and consistency with Federal, DoD, SECNAV, and USN policy and statutory authority using OPNAV 5215/40 Review of Instruction. This instruction will be in effect for 5 years, unless revised or cancelled in the interim, and will be reissued by the 5-year anniversary date if it is still required, unless it meets one of the exceptions in OPNAVINST 5215.17A, paragraph 9. Otherwise, if the instruction is no longer required, it will be processed for cancellation as soon as the need for cancellation is known following the guidance in OPNAV Manual 5215.1 of May 2016.

11. Forms and Information Management Control

a. OPNAV 5239/14 System Authorization Access Request Navy (SAAR-N) is available for download from Naval Forms OnLine, https://navalforms.documentservices.dla.mil/web/public/home.

b. Data collection contained in subparagraphs 8b(5), 8b(29)(h)(i), 8h(4), and 8q(8) is exempt from information management control per SECNAV M-5214.1 of 1 December 2005, part IV, subparagraph 7i.

Mall

M. J. KOHLER Deputy Chief of Naval Operations for Information Warfare

Releasability and distribution:

This instruction is cleared for public release and is available electronically only via Department of the Navy Issuances Web site, http://doni.documentservices.dla.mil

REFERENCES

- (a) DoD Instruction 8510.01 of 12 March 2014
- (b) SECNAVINST 5239.3C
- (c) SECNAVINST 5400.15C
- (d) 44 U.S.C. §3551, et seg, The Federal Information Security Modernization Act (FISMA) of 2014"
- (e) DoD 5220.22-M, National Industrial Security Program Operating Manual, 28 February 2006
- (f) SECNAVINST 5211.5E
- (g) DoD CIO Memorandum, Updated Guidance on the Acquisition and Use of Commercial Cloud Computing Services, 15 December 2014
- (h) E.O. 12333, United States Intelligence Activities
- (i) DoD Instruction 5200.01 of 21 April 2016
- (j) DoD Directive 5205.07 of 1 July 2010
- (k) DoD Instruction 5205.11 of 6 February 2013
- (1) SECNAVINST S5460.3H (NOTAL)
- (m) SECNAV M-5239.1 of 1 November 2005
- (n) SECNAVINST 5239.22
- (o) Committee for National Security Systems Instruction (CNSSI) 4009, Committee on National Security Systems Glossary, 6 April 2015
- (p) DoD Instruction 8115.02 of 30 October 2006
- (q) National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems: a Security Life Cycle Approach, 5 June 2014
- (r) NIST SP 800-82, Guide to Industrial Control Systems (ICS) Security, May 2015
- (s) NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, 22 January 2015
- (t) CNSSI 1253 Security Categorization and Control Selection for National Security Systems, 27 March 2014
- (u) NIST SP 800-53A, Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans, 18 December 2014
- (v) Navy Telecommunications Directive (NTD) 11-08, Electronic Spillage Requirements
- (w) DoD Directive 8140.01 of 11 August 2015
- (x) SECNAV M-5239.2 of 27 June 2016
- (y) DoD Instruction 8500.01 of 14 March 2014

- (z) UNSECNAV Memorandum, Organizational Realignments and Designation as the Department of the Navy Deputy Chief Information Officer (Navy) and the Department of the Navy Deputy Chief Information Officer (Marine Corps), 11 May 2011
- (aa) Joint CNO/ASN RDA Memorandum, Navy Information Technology Technical Authority, 9 October 2012
- (ab) OPNAVINST N9210.3 (NOTAL)
- (ac) OPNAVINST 5450.345
- (ad) DoD Directive 5240.06 of 17 May 2011
- (ae) CJCSI 6510.01F
- (af) COMOPTEVFORINST 3980.2H
- (ag) SECNAVINST 5000.2E
- (ah) DoD Instruction 8530.01 of 7 March 2016
- (ai) OPNAVINST F3100.6J (NOTAL)
- (aj) DoD Instruction 8520.03 of 13 May 2011
- (ak) SECNAVINST 5510.36A
- (al) DoD Instruction 5000.02 of 7 January 2015
- (am) Chairman of the Joint Chiefs of Staff Manual for the Operation of the Joint Capabilities Integration and Development System (JCIDS) of 12 February 2015
- (an) DoD Program Manager Guidebook for Integrating the Cybersecurity Risk Management Framework into the System Acquisition Lifecycle, 27 October 2015
- (ao) 48 CFR 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- (ap) NIST SP 800-171, Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations, June 2015
- (aq) OPNAVINST 5450.343
- (ar) OPNAVINST 5450.353
- (as) SECNAVINST 5239.20A
- (at) SECNAV WASHINGTON DC 051800Z JAN 16 (ALNAV 001/16)
- (au) SECNAVINST 5510.37
- (av) DoD Information Systems Agency Enclave Test and Development Security Technical Implementation Guide (STIG), Version 1, Release 3, 22 January 2016
- (aw) VS-JI-22A, Virtual SYSCOM Engineering and Technical Authority Policy, 31 January 2007 (NOTAL)

RISK MANAGEMENT FRAMEWORK TAXONOMY

1. Introduction

a. This document establishes taxonomy, defines detailed constructs, and establishes high level procedural guidance for the USN's execution of reference (a).

b. The USN implementation of the risk management framework will utilize a construct that recognizes the imperatives of network security and management of community risk while ensuring accountability for mission capability and leveraging mission area domain-expertise. This taxonomy will define a hierarchical risk management framework assessment and authorization process and structured cybersecurity risk assessment process that aligns with risk management framework, the Navy program budget, and the TA and FAO constructs.

c. With the understanding that the DoDIN exists to support the DoD mission areas, Navy must create a construct that recognizes the importance of mission requirements while respecting the ubiquitous nature of cyber threats and complies with reference (y).

d. Reference (m) states that cybersecurity will be achieved through the cost-effective, risk-balanced application of controls in a manner that promotes confidentiality, integrity, availability, non-repudiation, and authentication of information. Personnel responsible for development, acquisition, assessment, authorization, fielding, and operation of USN IT assets must respect and adhere to these basic tenets of cybersecurity when executing their respective duties.

e. Per reference (o), to further delineate the distinction between CND, DCO, and cybersecurity the DoD distinguishes each as follows:

(1) Per reference (0), CND and DCO consist of the operational and personnel measures taken to defend against unauthorized activity within computer networks. This includes monitoring, detection, analysis (such as trend and pattern analysis), and response and restoration activities.

(2) Per reference (o), cybersecurity consists of the technical and managerial measures that protect and defend information and IS by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities. Further, USN specifically includes disaster recovery and continuity of operations as technical and managerial measures.

(3) The five attributes of cybersecurity, defined in references (m) and (o), are per subparagraphs le(3)(a) through le(3)(e).

(a) <u>Confidentiality</u>: Assurance that sensitive information is preserved and not disclosed to unauthorized system entities (users, processes, or devices). This includes the protection of operational information, cybersecurity-related system information, and CUI, to include personally identifiable information and proprietary information.

(b) <u>Integrity</u>: Assurance that information and systems are not modified by unauthorized parties or in an unauthorized manner. Integrity supports the assurance that data and information are not accidentally or maliciously manipulated, altered, corrupted or destroyed (includes ensuring information non-repudiation and authenticity).

(c) <u>Availability</u>: Timely, reliable access to data and information services by authorized users.

(d) Authentication

 $\underline{1}$. The substantiation of the identity of a message sender or receiver.

 $\underline{2}$. A security measure designed to verify the identity or other attributes claimed by or assumed of an entity (user, process, or device) or to verify the source and integrity of data.

<u>3</u>. A means of verifying an individual's authorization to receive specific categories of information.

(e) <u>Non-repudiation</u>: Assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data. Additionally, nonrepudiation is protection against an individual falsely denying having performed a particular action. Non-repudiation provides the capability to determine whether a given individual took a particular action such as creating information, sending a message, approving information, and receiving a message.

2. Structure

Reference (a) designates the SECNAV as responsible for a. the full implementation of risk management framework within the DON. Per reference (z), SECNAV has delegated specific responsibilities to CNO (N2N6) as the DDCIO(N). In the DON CIO memorandum "Designation of Department of the Navy Deputy Senior Information Security Officers (DDSISO)" of 12 November 2015, DON CIO designated the DDCIO(N) as the DDSISO(N). The DDSISO(N) is responsible for the administration of the risk management framework within the USN cybersecurity program; participation in the Risk Management Framework Technical Advisory Group; visibility and sharing of the risk management framework status of assigned IT; and enforcement of training requirements for persons executing duties specific to the risk management framework.

b. Commander, FLTCYBERCOM is designated as the NAO. The NAO role at FLTCYBERCOM will manage and maintain oversight over community risk and the DoDIN.

c. To enable accountability for safety, mission areas, products, platforms, and facilities; Commanders, NAVSEASYSCOM, NAVAIRSYSCOM, NAVFACENGCOM, and SPAWARSYSCOM, and Director, SSP are assigned as FAOs for all IT under their purview as defined in paragraph 3 of this enclosure, the AO determination guide.

d. As part of the SYSCOM platform assessment, the SYSCOM commander will ensure a platform cybersecurity risk assessment is performed. The platform cybersecurity risk assessment will be conducted in conjunction with the SCA representative to evaluate at the platform level the aggregated cybersecurity risks from each of the enclaves of systems.

e. SPAWARSYSCOM, as the cybersecurity TA, will:

(1) provide mandatory training and certification for all SCAs, including validators;

(2) establish, implement, and monitor a process that ensures individuals executing the SCA duties hold the appropriate technical warrants; and

(3) develop standard technical processes, tools, technical implementation standards, and risk management framework templates.

f. Oversight and Compliance

(1) The AO Council (charted in paragraph 7 of this enclosure) will be responsible for the establishment and oversight of a review team to ensure consistent application of, and adherence to, technical processes and standards approved by DDCIO(N) or the IT/CS TAB.

(2) This review team will consist of:

(a) SPAWARSYSCOM, as the cybersecurity TA, to colead all technical reviews;

(b) members from each FSCA, to co-lead the reviews for their respective systems; and

(c) members from each AO, to assist as required.

(3) The review team will be responsible for:

(a) review of packages' end-to-end risk management
framework process;

(b) identification of common deficiencies with corresponding remediation recommendations;

(c) escalation of unfavorable process findings;

(d) review of systems' continuous monitoring
programs to ensure they remain compliant and are repeatable and
sufficient;

(e) ensuring risk management framework package returns are for only substantive reasons (not administrative) and that these reasons are clearly articulated with the returns; and

(f) ensuring cybersecurity inspection results are incorporated into the risk management framework process.

(4) The cybersecurity TA will report all findings to the AO Council twice a year or as the AO Council requires.

3. <u>AO Determination Guide</u>. This paragraph defines who will be the AO for systems in all possible scenarios.

a. Systems that handle SCI or SAP data are under the respective jurisdictions of the NIA and OPNAV N9SP.

b. All IT determined to contain high or very high system risk during step 4 in reference (a) will require the signature approval of DON CIO before issuance of an authorization by the cognizant AO through the codified DON CIO High Risk Escalation Standard Operating Procedure of 18 May 2016.

c. All IT with direct connections to the Defense Information Systems Network (DISN) must be authorized by signature of the NAO. Any IT that was formerly authorized by a FAO that is seeking to connect to the DISN will follow DDCIO(N) guidance to renew their ATO under NAO's cognizance. This will be done per the requisite memorandums of understanding between the respective program, FAO, and the NAO.

d. Non-DoD IT as well as all IT not under the jurisdiction of an FAO will be assessed by the Navy SCA and authorized by signature of the NAO.

e. NAVAIRSYSCOM, NAVFACENGCOM, NAVSEASYSCOM, SPAWARSYSCOM, and SSP will serve as FAOs for aviation, facilities, surface, subsurface, and space platforms IT aligned to the assigned TA as defined by reference (c) and assigned by CNO (N2N6). These FAOs will be the AOs for all IT under their purview that are not excepted by any aforementioned clauses.

f. Research, development, test, and evaluation (RDT&E) zone A, the primary test and development and external node connection, will be authorized by the NAO based on a security control assessment by the appropriate SCA. Echelon 2 commands with FSCA authority will serve as SCA for Zone A. Echelon 2 commands without FSCA authority will use the Navy SCA.

g. RDT&E zones B, C, and D enclaves will be authorized by their respective FAO based on security control assessment by the FSCA. The authoritative definitions of RDT&E zones can be found in reference (av). A brief overview to assist in AO identification is below per subparagraphs 3g(1) through 3g(4).

(1) Zone A environments have direct connectivity to external DoD networks. They are typically configured as mirrored operational networks for final end stage testing. This environment will have connectivity to the live operational network for final data testing prior to the product or application deployment into the operational network.

(2) Zone B environments have indirect controlled connectivity to external DoD networks. They are environments which are the designated zone permitting connectivity for moving sanitized data for testing purposes along with development of applications destined for a live and operational DoD network. Testing and evaluation within the environment includes nonpersistent systems with limited activity and connectivity on the network. Logical or physical separation is acceptable to keep systems from accessing any development areas within the environment. Products, applications, or other systems tested in these environments will have prohibitive access controls to DoD operational networks. Zone B environments receive all networking and cybersecurity services from production, zone A, and core networks. The definition of a zone B enclave is a far more intricate and sensitive one than the other zones - it is highly recommended to refer directly to reference (av) prior to designating an enclave as zone B, especially as it pertains to the use of virtual private networks and connectivity restrictions.

(3) Zone C environments are interconnected enclaves logically isolated from external DoD networks. They are specific in nature to organizations that have a mission to interconnect with other organizations to create a fully closed

multi-environment network for product testing and evaluation. The network is isolated from the rest of an organization's operational network. Direct access to the DISN is not permitted for zone C environments as the DISN is used to transmit data between environments.

(4) Zone D environments are physically isolated enclaves with no connectivity to external DoD networks. They are fully closed and physically separate from any DoD live operational network.

h. Per reference (y), ATOs for CDS are dependent on the approval of a CDS authorization by the DoD Information Security Risk Management Committee or one of its delegate committees, such as the Defense Security/Cybersecurity Authorization Working Group.

i. Dispute resolution will be executed per the AO Council charter (found below in paragraph 7).

4. <u>AOs' Responsibilities and Requirements</u>. For all IT assets under their respective jurisdictions, AOs will perform the responsibilities contained in this paragraph.

a. Grant an ATO, ATO with conditions, or interim authorization to test of a network or system depending on the environment and intended use of the respective asset along with its associated risk posture.

b. Issue a denial of ATO of a network or system that poses an unacceptable risk or that is being decommissioned.

c. Determine the final operational risk of USN IT being authorized and accept residual risk.

d. Ensure cybersecurity TA standards and continuous monitoring are incorporated as elements of the IT life-cycle process.

e. Ensure the operational IT security policies are in place for each system, project, program, and organization or site for which the AO has authorization authority.

f. Ensure the establishment, administration, implementation, and coordination of security for systems that the AO's command or organization operates.

g. Coordinate defense information infrastructure connection approval with DISA for USN IS and sites. Ensure sites with defense information infrastructure connections meet DISA accreditation requirements. Utilize COMOPTEVFOR as the operational test agents as applicable and where necessary.

h. Execute AO authorities, as designated by non-Navy entities and mission owners (e.g., U.S. Strategic Command). All designations must be coordinated through CNO (N2N6).

i. Participate in the AO Council and ensure that unresolved issues are escalated to DDCIO(N).

j. Validate the operational requirement for internal echelon 2 CDS requests.

k. Provide AO first endorsement of CDS requests from external echelon 2s.

1. Provide annual AO validation to continued operational requirement for CDSs to DISA.

m. Verify operational enclaves and Navy unique CDS have a current accreditation and resolve accreditation issues with the appropriate echelon 2 CIO.

n. Identify all direct or indirect cross domain connections and verify appropriate DoD IC authorization for operational use.

o. Ensure all USN IT is properly categorized.

p. Ensure all USN IT maintain current authorization or assessment approval.

q. Ensure agreements are established among the AOs and documented in the security plan when systems involve multiple AOs.

r. Ensure all USN IT with conditional authorizations submit and comply with plans of action and milestones and associated timelines.

s. Submit all requests for continued operation of systems and circuits with high or very high residual risk to DDCIO(N) for endorsement and forwarding to DON CIO for final approval as part of the high risk escalation process.

t. Serve as one of the testing agents with COMOPTEVFOR as part of risk analysis and mitigation for new equipment and networks prior to fleet deployment and AO accreditation, following the role specified in reference (ae). This testing agent role is different than an SCA role.

5. SCA Responsibilities and Requirements

a. SCAs will, for all IT assets under their respective jurisdictions, perform the following responsibilities contained in subparagraphs 5a(1) through 5a(7).

(1) Provide risk management framework compliant risk assessments and recommendation correspondence to the appropriate AO.

(2) Assess and approve the risk management framework security assessment plan.

(3) Assess the management, operational, and technical security controls.

(4) Validate that the controls are:

- (a) implemented correctly;
- (b) operating as intended; and
- (c) producing the desired outcome.

(5) Assess the severity of weaknesses or deficiencies in the security authorization package.

(6) Assist the ISSM and IS security engineer in determining corrective actions to address identified vulnerabilities.

(7) Prepare the final security assessment report containing the results and findings from the assessment.

b. Assessor and validator independence is an important factor in:

(1) preserving the impartial and unbiased nature of the assessment process;

(2) determining the credibility of the security assessment results; and

(3) ensuring that the AO receives the most objective information possible in order to make an informed, risk-based, authorization decision.

6. Specific AO and SCA Command Responsibilities

a. FLTCYBERCOM

(1) Commander, FLTCYBERCOM will serve as the NAO.

(2) The NAO will publish:

(a) the process for systems transitioning fromDIACAP to risk management framework;

(b) the process for tracking ATOs for all IT assets including plans of action and milestones to include active engagement with stakeholders of expiring systems; and

(c) the process for promoting reciprocity from non-USN platforms and systems as receiving and deploying organizations following reference (a). This includes establishment of a reciprocity and control inheritance escalation process.

b. NAVAIRSYSCOM

(1) Per references (c) and (aw), NAVAIRSYSCOM is the TA for air systems, aeronautical weapons systems and associated subsystems, support equipment, components and parts, systems integration, software, and human systems.

(2) NAVAIRSYSCOM TA responsibilities will include:

(a) oversight of core processes required to support the acquisition, in-service support and disposal of air systems;

(b) operation and sustainment of the most efficient infrastructure needed to acquire, field, and support air systems;

(c) establishment of standard policies, technical specifications, and processes;

(d) introduction of advanced technology and lessons learned; and

(e) providing trained and qualified personnel, per references (w) and (x), to the integrated program teams.

(3) For in-service systems, NAVAIRSYSCOM has jurisdiction over all aircraft equipment limitations and technical data in Naval Air Training and Operating Procedures Standardization, Naval Aviation Technical Information Product publications, and airworthiness certification of all naval aircraft.

c. NAVFACENGCOM

(1) Per references (c) and (aw), NAVFACENGCOM is the TA for all matters relating to facilities engineering policies and practices. Specifically, NAVFACENGCOM manages and executes the planning, design, construction, and public works support for naval facilities on a worldwide basis.

(2) NAVFACENGCOM TA responsibilities will include:

(a) oversight of core processes required to support the acquisition, in-service support and disposal of ashore infrastructure;

(b) operation and sustainment of the most efficient infrastructure needed to support the USN ashore mission; and

(c) establishment of standard policies, technical specifications, and processes.

d. NAVSEASYSCOM

(1) Per references (c) and (aw), NAVSEASYSCOM is the TA for ships and ship systems.

(2) NAVSEASYSCOM TA responsibilities will include:

(a) oversight of core processes required to support the acquisition, in service support and disposal of platforms;

(b) operation and sustainment of the most efficient infrastructure needed to acquire, field, and support weapon systems and commodities;

(c) establishment of standard policies, technical specifications, and processes;

(d) rapid and consistent incorporation of advanced technology and lessons learned; and

(e) support for integrated platform management teams.

e. SSP

(1) Per references (c) and (aw), SSP is the TA for seabased deterrent missile systems.

(2) SSP TA responsibilities will include:

(a) oversight of core processes required to support the acquisition, in-service support and disposal of platforms;

(b) operation and sustainment of the most efficient infrastructure needed to acquire, field, and support weapon systems and commodities;

(c) establishment of standard policies, technical specifications, and processes;

(d) rapid and consistent incorporation of advanced technology and lessons learned; and

(e) support for integrated platform management teams.

f. SPAWARSYSCOM

(1) Per references (c) and (aw), SPAWARSYSCOM is the TA for command and control systems, communication systems, intelligence systems, space systems, force level warfare systems architectures, and FORCEnet. Additionally, SPAWARSYSCOM is the command, control, communications, computers, and intelligence chief engineer to all other SYSCOMs, having oversight over any command, control, communications, computers and intelligence engineering related activity.

(2) SPAWARSYSCOM must also serve as Navy SCA for assigned systems as required.

(3) SPAWARSYSCOM must provide risk management framework compliant risk assessments and certification recommendation correspondence to the NAO.

7. AO Council Charter

a. <u>Purpose</u>. This establishes the AO Council as the senior level decision body within the Navy's risk management framework implementation to ensure enterprise awareness; coordinate interdomain decisions; review ongoing threats, trends, and inspection results; and adjudicate differences amongst peer AOs with regard to risk decisions.

b. Council Responsibilities. The AO Council will:

(1) be the authoritative decision making body for all USN risk management framework authorization disputes for IT under the cognizance of the NAO or FAOs;

(2) advise the DDCIO(N) and the Navy Enterprise Information Technology Governance Board and recommend modifications to existing risk management framework policy and authorization procedures; and

(3) be responsible for the establishment and oversight of the review team described in subparagraph 2f(2) of this enclosure.

c. <u>Membership</u>. The AO Council will be FO and SES level principal (required attendance) and adjunct (optional attendance) members. When alternate participation is required, principal members will ensure senior level representation is maintained. Adjunct members will be allowed to fully participate in all meetings. While consensus will be sought in decisions and recommendations pursued by the council, consensus is not required. At the discretion of the DDCIO(N), unresolved issues may be raised to the Navy Enterprise Information Technology Governance Board for resolution.

(1) <u>Principal Members</u>. Principal members include FO and SES level representatives from the following organizations listed in subparagraphs 7c(1)(a) through 7c(1)(g).

- (a) DDSISO(N) AO Council chair
- (b) FLTCYBERCOM (NAO)
- (c) NAVAIRSYSCOM (FAO)
- (d) NAVSEASYSCOM (FAO)
- (e) NAVFACENGCOM (FAO)
- (f) SSP (FAO)
- (g) SPAWARSYSCOM (FAO)

(2) <u>Adjunct Members</u>. Adjunct members include FO and SES level representatives from the following organizations listed in subparagraphs 7c(2)(a) through 7c(2)(f).

(a) SPAWARSYSCOM as the cybersecurity TA

- (b) USFLTFORCOM
- (c) COMPACFLT

(d) Deputy Assistant SECNAV (DASN) Command, Control, Communications, Computers and Intelligence/Space

- (e) Resource sponsors
- (f) DON CIO.

(3) <u>AO Council Chair</u>. DDSISO(N) will serve as the AO Council chair.

(4) <u>AO Council Secretariat</u>. Director of Navy Cybersecurity and CIO (OPNAV N2N6G) will serve as the secretariat for the council.

(5) <u>AO Coordination and Synchronization Working Group</u>. This working group will be comprised of a standing group of O-6 and GS-15 representatives of principal and adjunct member organizations and chaired by a DDSISO(N) representative. The group will meet quarterly, though additional meetings may be scheduled at the discretion of DDSISO(N).

(6) <u>Sub-working Groups</u>. As directed by the AO Council, sub-working groups will be established temporarily or permanently to facilitate and address specific issues or processes.

- d. Roles
 - (1) AO Council Chair

(a) Be the final decision making authority, adjudicating and resolving disputes between AO Council members when consensus cannot be reached.

(b) Add or change adjunct members, or invite one or more individuals to attend specific meetings for the purpose of providing relevant information or expertise to assist in the council's deliberations.

(2) AO Council Secretariat

(a) Call and administer AO Council meetings.

(b) Review risk management framework issues, problems, and equities presented during council meetings to facilitate adjudication of differences between AOs.

(c) Review and approve council meeting minutes.

(d) Assemble, prepare, and distribute read-ahead material prior to the scheduled meetings on matters under consideration by the council.

(e) Publish time and location for upcoming meetings and advise members accordingly.

(f) Post agendas for council meetings within 1 week of scheduled date.

(g) Disseminate decisions and actions reached by the council within 5 days of meeting.

(h) Track council actions and decisions through resolution, and provide venue for DDCIO(N) to monitor progress on council actions and decisions.

(i) Collaborate, coordinate, and exchange information with secretariats of other relevant organizational groups under the guidelines established by the council.

(3) Council Members

(a) Attend all council meetings or designate an appropriate FO or SES alternate representative.

(b) Identify and nominate agenda items to the AO Council chair for review and vetting.

(c) Represent member's organization, providing feedback or recommended actions proposed or being considered by the council.

(d) Represent the positions and decisions of the council to their organizations.

(e) Execute actions and tasks as agreed to by the council.

(f) Ensure their organizations participate on appropriate sub-working groups.

(g) Review council meeting minutes.

(4) AO Coordination and Synchronization Working Group

(a) Serve as the lead coordination group for the AO Council.

(b) Prepare or review required read ahead material for each council meeting.

(c) Provide situational awareness of risk management framework governance specific items and areas of interest to the leadership of their respective organization.

(d) Provide recommendations to the council on the establishment of sub-working groups as necessary to address items and areas of interest.

(e) Develop required assessments and advise the member organization leadership on proposed guidance and actions recommended by the council.

(f) Exhaust all attempts to resolve disputes before elevating issues to the formal AO Council.

(5) Sub-working Groups

(a) Research, analyze, coordinate, and adjudicate recommendations for the issues within the sub-working groups' tasked AOR.

(b) Brief the council, represented organizations, and board members on sub-working group recommendations.

e. Meeting Procedures

(1) AO Council meetings will be held at the request of any primary member or in the event that the AO coordination and synchronization working group is unable to reach a decision on an issue. These meetings may be held in person, via teleconference, video teleconference, or Defense Collaboration Services.

(2) Council attendance is limited to the FO and SES members and to necessary subject matter expert attendees.

f. <u>Review and Cancellation</u>. This charter will be reviewed annually and will remain in effect until cancelled.