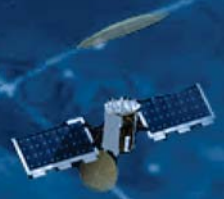
Space and Naval Warfare Systems Command



Strategic Plan

Execution Year 2016

SPAWAR

Rapidly Delivering Cyber Warfighting Capability from Seabed to Space

SPAWAR Strategic Plan

Execution Year 2016

FOREWORD

The SPAWAR Strategic Vision 2015-2022 describes the long range end-states that we must achieve to fully align to the Navy's mission and support and empower our warfighters in the cyber domain. Throughout 2015 we worked on key objectives to support those end-states. Informed by this foundational work and Chief of Naval Operations (CNO) guidance, *A Design for Maintaining Maritime Superiority*, the SPAWAR Strategic Plan further refines our course to achieve the SPAWAR Vision.

2015 key accomplishments include:

Accelerate & Streamline Delivery

- Aligned twenty-five DDG availabilities (FY18-FY22) to a synchronized fielding plan, baseline definition decreased guided missile destroyer C4I configurations
- Completed the Romania Aegis Ashore site C4I installation and INSURV acceptance trials in advance of the presidential mandated 31 Dec 2015 Aegis Weapon System Full Operational Capability
- Successfully launched and placed in operational orbit Mobile User Objective System (MUOS) satellites 3 and 4
- Established a comprehensive and executable plan to enhance ship installation performance
- Established a cross-enterprise working group to develop requirements to accelerate advanced technology delivery
- Initiated SPAWAR scheduling policy to leverage modern applications and analytics tools
- Reduced Consolidated Afloat Networks and Enterprise Services (CANES) aircraft carrier installs: 14 months down to seven months in one year
- Completed comptroller CANES installation cost study
- Started regular, formal government-industry reviews
- Fielded an integrated management scheduling tool for contracts and PEOs

Enable Modern IT Service Delivery

- Achieved the Navy's Cloud Access Point initial operational capability, a critical first step in enabling the use of commercial cloud providers
- PEO EIS Innovation Cell successfully tested rapid Information Technology (IT) acquisitions and is on track to complete two full rapid acquisitions (concept to delivery) in less than one year
- Completed assessment of application cloud readiness phase I by categorizing Navy systems security and information impact level, and completed assessment of phase II for business systems
- Started Hyper Converged Infrastructure (HCI) pilots
- Fielded more than 17,000 iPhone devices, dramatically increasing user capability and satisfaction
- Conducted two commander's forums on sustainment reviews
- Completed competition and subsequent award of unified military medical records management system

Own Cyber Technical Leadership

- Cross-SYSCOM Technical Authority Board signed off on eight technical cybersecurity standards
- Cross-SYSCOM Technical Authority Board developed and is reviewing cyber risk assessment standard
- Established a technical approach for the Navy's CYBERSAFE initiative and completed the first multidiscipline CYBERSAFE pilot
- Implemented cyber dashboards to document and provide ship's force and type commander's (TYCOM) insight to assess cyber hygiene compliance on 31 fleet units.
- Supported Cyber Security Inspections (CSI), Command Cyber Readiness Inspections (CCRI) and development of new CSI 2.0 inspection criteria
- Established Fleet, TYCOM, Fleet Cyber Command (FCC) and SPAWAR working group agreement on specific data elements that are within TYCOM and afloat site capability and capacity to manage in a repeatable and executable process
- Led Navy-wide efforts and trained multiple organizations (NAVSEA, NAVAIR, CNAF, CNAL, CNSF, CNSL, IDFOR, FCC) to optimize the use of Vulnerability Remediation and Management (VRAM) to increase Navy proficiency in reducing network vulnerabilities
- Helped define the Navy Joint Regional Security Stacks (JRSS)/Joint Information Environment (JIE) architecture
- SPAWAR selected to be the Nuclear Command, Control, and Communications Chief Engineer (NC3 CHENG)
- Began work on redefining SPAWAR 5.0's architecture authority
- Began implementation of Risk Management Framework (RMF)

Reduce the Cost of Operations:

- Began developing a data-driven culture through the collection, development and increased use of headquarters data
- Selected and began migration to an enterprise Business Intelligence (BI) architecture; this migration will result in a reduction of the three BI silos as well as provide the platform for future enterprise reporting capabilities
- Avoided an estimated $12.4M per year of program costs by reducing the FY17 Navy Working Capital Fund composite rate below FMB's inflation guidance
- Re-established the cross-command efficiencies IPT to identify and initiate cost savings recommendations, in response to workforce-generated suggestions: (1) consolidated government purchase card approving officials and card holders across headquarters, (2) reduced and restructured services contracts, (3) replaced the Information Technology Procurement Request (ITPR) process using existing Navy ERP data systems and IT spend plan processes, and (4) revised the justification and approval process for sole source hardware and software procurements
- Developed long-range contracting opportunities acquisition forecast as part of a continued effort to reduce the time and expense of contract management activities
- Updated policy for conducting procurement schedule meetings
- Updated acquisition milestone scheduling templates and tools

Optimize Our Organization & Workforce:

- Realigned the organizational billet structure to support increased FY17 reductions
- Developed cyber training for non-cyber acquisition workforce
- Implemented SPAWAR Cyber Warrior training for new employee orientation
- Identified modern information-related requisite skillsets and initiated SPAWAR training, hiring, competency development, and talent management analysis
- Implemented project management requirements throughout Installation Management Offices (IMO)
- Consolidated five SATCOM system In-Service Engineering Agents (ISEAs) under one unified capability-based ISEA, lessons learned will enable the consolidation of an additional 52 system ISEAs into 16 Capability ISEAs by the start of FY17
- Implemented an HQ-wide iMentoring program
- Implemented a new leadership development program and convened the first class
- Realigned SPAWAR OIC billets by port and streamlined their chain of command to support new IMO structure
- Gained authority to award Enlisted Information Warfare qualifications
- Implemented a coherent SPAWAR Systems Center non-Navy work divestment plan

We made significant progress in 2015 but much work remains. The SPAWAR Strategic Plan further develops and refines the discrete objectives and gives us the added structure necessary to achieve the end-states identified in our Vision. These objectives align with the Navy's mission, and are supported by executable measures and milestones. Our progress on each of these objectives will describe our performance as an organization and the value of our support to the Navy warfighter.

Both the SPAWAR Vision and Strategic Plan were developed with expertise from across the organization. This must remain a "living document". As the cyber environment evolves, priorities shift or as objectives are achieved, we must be prepared to adjust to these changes. A detailed understanding of our progress towards our objectives is fundamental to maintaining this agility. A robust and transparent execution management strategy is critical for success.

Ultimately, achieving our vision through our strategic plan is dependent on every member of our civilian, military and contract support workforce. It is vital we appreciate how every competency, workcenter and individual contributes to our mission. Together, as one team, the Navy depends on us to *rapidly deliver cyber warfighting capability from seabed to space*.

Rear Admiral David H. Lewis,
Commander,
Space and Naval Warfare
Systems Command

Mr. Patrick Sullivan,
Executive Director,
Space and Naval Warfare
Systems Command

SPAWAR Strategic Plan

Execution Year 2016

Achieving the SPAWAR Vision 2015 - 2022

VISION OVERVIEW

Foundational Principles

RELEVANT - We will assess our progress and adjust as required in order to provide secure, affordable and unparalleled cyber capabilities in and through a dynamic cyber operational environment.

RESILIENT - We build tough systems that deliver interoperable, intuitive and reliable capabilities by establishing and adhering to effective cyber architectures.

RESPONSIVE - We take the initiative and remain agile. We are accountable to solve tough problems and deliver innovative solutions that enable decisive operational advantage.

SPAWAR's vision is to rapidly deliver cyber warfighting capability from seabed to space. This vision is relevant to the entire SPAWAR enterprise, including SPAWAR Headquarters, our supported Program Executive Offices, the SPAWAR Systems Centers, and the SPAWAR Space Field Activity. To achieve this vision, we must continue to build a world class team that is focused on leveraging technology to equip our warfighters with systems that enable our dominance of the cyber domain. We must deliver systems that are unmatched in the world and affordable across their lifecycle. SPAWAR products must be secure, reliable and intuitive. They must be interoperable across the fleet and agile in addressing threats that are changing with unprecedented speed.

When we use the term cyber, we mean the all-encompassing domain of or related to computing, with networked capability that has been extended to provide a decisive advantage over our adversaries. This capability now extends to the very core of our nation's warfighting systems and our platforms' most basic functions like machinery control, navigation and weapon systems.

While we have unprecedented control and management of our systems and platforms, we are also more dependent on networked and computer-controlled systems than ever before. These critical systems are vulnerable to cyber attack. We need to recognize the extent of these vulnerabilities and develop positive steps to counter them.

Our dependency on cyber for daily activities and warfighting advantage has revealed a new warfighting domain. Cyberspace is the 5th warfighting domain and stands on par with the physical domains of land, sea, air and space. In the cyber domain, information is created, transported and processed. This includes the ability to observe the physical domains, turn these observations into actionable intelligence and command decisions, and exert precise control of our advanced weapon systems. Information warfare is enabled by, and delivered through, technical capabilities based in the cyber domain. The Navy continues to integrate cyberspace operations as an essential component of fleet operations. Effective, assured cyber operations must become part of our core mission to maintain our warfighting advantage.

Our maneuver operations occur in the cyber battlespace comprised of networked systems and the electromagnetic spectrum. SPAWAR must ensure the Navy maintains its cyber advantage by providing capability to observe activity across all domains, including the electromagnetic and information environments. SPAWAR maintains the full spectrum of connectivity required for modern naval warfare.

We will deliver capabilities that turn observations into actionable intelligence and support command and control of naval forces in all five warfighting domains. We will provide the technical capabilities to operate and maneuver (to protect, detect and respond) in the cyber and electromagnetic environment by delivering advanced cyber capability to the warfighter.

To succeed we will expand the knowledge of cyber operations throughout our workforce. We will optimize our organization to maximize agility and effectiveness in the face of an evolving threat. We will research and develop capabilities to visualize and conduct real-time operations in the cyber domain. We will ensure that we can operate our information and computer controlled systems in dynamic environments.

In delivering these capabilities, fiscal realities will challenge us to remain lean and focused. Regardless of budget challenges, we will innovate and provide the absolute best value to the warfighter for each taxpayer dollar.

To achieve this vision, we must:

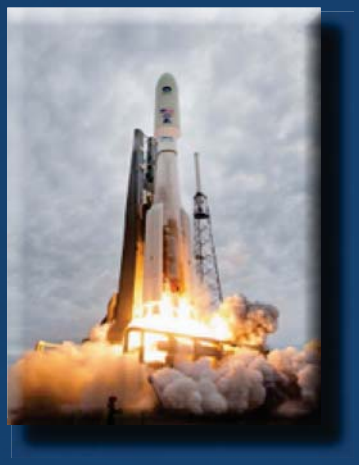
1. **Accelerate and streamline delivery** of new capability and advanced technology to the fleet to maintain U.S. technological superiority and to maximize warfighter advantage.
2. **Enable the delivery of advanced modern IT and cyber capabilities** and transform what it means to operate and maneuver within the cyber domain.
3. **Provide the cyber technical leadership** required across the Navy.
4. **Reduce the cost of operations** to ensure delivery of affordable warfighting solutions.
5. **Optimize our organization and workforce** to bring about this change.

This strategic plan provides the milestones, measures of performance and measures of effectiveness for each of our strategic objectives. The targeted end-states associated with these tasks align with Chief of Naval Operations (CNO) guidance and are supported by specific and measurable objectives to ensure we remain on course toward our vision as an organization.This guidance frames the problem and a way forward while acknowledging that there is inherent and fundamental uncertainty in both the problem definition and the proposed solution. We will continually assess the environment, to ensure that we respond in a way that is consistent with achieving our goals. This strategic plan will guide our behaviors and investments, both this year and in the years to come.

The targeted end-states associated with these tasks align with CNO guidance and are supported by specific and measurable objectives to ensure we remain on course toward our vision as an organization. This strategic plan provides the milestones, measures of performance and measures of effectiveness for each of those strategic objectives.

ACCELERATE AND STREAMLINE DELIVERY

Driving down cost and decreasing the time it takes to provide new capability to the fleet must be foremost in our approach. We must deliver cyber capability in a way that ensures interoperability, operational availability and the ability of our Sailors to develop and sustain proficiency in operations and maintenance. We must design our systems in a way that makes them easy to install and upgrade. We must evaluate the quality of the products we are procuring and leverage automated testing tools.



Objective 1.A: Increase Commonality in Deployed C4I Configurations

This objective focuses on efforts to increase commonality in deployed C4I configurations while delivering maximum warfighter capability and increased operational availability. PEO C4I will define C4I capability baselines for all classes of ships based on the mission requirements, ensuring the deployed operational capability matches the warfare requirement. C4I capability baselines will be maintained for groups of ships over multiple years in alignment with the Optimized Fleet Response Plan (O-FRP) needs. C4I capability baselines are integrated capabilities which include configuration management artifacts, system of systems testing, baseline persistent monitoring, cyber compliance assessment, and capability based training. Implementation of C4I capability baselines will increase warfighters ability to operate and maintain systems while reducing support costs. Operators and maintainers will be more capable of performing their system of systems functions that enable information warfare capabilities.

Delivery of operational capabilities, with proven performance and support will be accelerated with improved pre and post installation configuration management, cyber compliance, testing, and training. Consistent delivery of managed baseline configurations will streamline delivery due to the consolidation of Installation Management Office (IMO) contracts and increased Alteration Installation Team (AIT) familiarity with baseline installs.

MILESTONES

Prepare C4I baseline wholeness fielding plans and insert into PB17 synchronized fielding plan process (CY2016)

Conduct Mulit-TADIL Joint (MTJ) train-the-trainer seminars and user documentation validation for Ballistic Missile Defense Tactical Digital Information Link (BMD TADIL) operators (CY2016)

Conduct PEO C4I product roadmap reviews with Deputy PEO for Modernization (CY2016)

Approve DDG (BMD) C4I Baseline E2C Event Management Plan FY17 by PEO C4I Portfolio Governance Board (CY2016)

Produce MTJ Personnel Qualification Standards and submit to Naval Education and Training Command (NETC) (CY2016)

Produce DDG (Lead Class) Baseline Engineering Change Request (ECR) for review by Platform Technical Review Board (CY2016)

Coordinate C4I Baselines POM19 Input (CY2016)

Execute DDG C4I E2C Operational Capability Build (OCB) Test Sequences (CY2016)

MEASURES OF PERFORMANCE:

- Number of platforms (or platform avails) planned to receive a C4I capability baseline (as reflected tri-annually in the synchronized fielding plan)
- Number of operational capability builds derived test sequences tested prior to install
- Number of operational capability builds derived test sequences tested post install
- Number of operational capability builds derived test sequences not tested

MEASURES OF EFFECTIVENESS:

- Percentage of procurement budget aligned / not aligned to fielding complete C4I capability baselines
- (Future) Percentage of in-service DDGs in a C4I baseline executed vs. planned by fiscal year
- (Future) Number of unique DDG C4I configurations executed vs. planned by fiscal year
- (Future) Number of CASREPs for C4I technical assistance filed by platforms under C4I baseline
- (Future) Number of Fleet Systems Engineering Team (FSET) assists to C4I baseline platforms compared to FSET assists to non-C4I baseline platforms

Objective 1.B: Improve the Design for Installations & Decrease Installation Timelines & Cost

Installation timelines can be reduced through a combination of near term installation process improvement opportunities including: system design requirements that drive C4I systems to enable modernization; in-rack component level replacements; and, both technical and process changes to reduce touch time on ships for software installation.

Key focus areas for this objective are:

- Increase overall efficiency of SPAWAR installations with focus on affordability
- Increase transparency by providing standardized reports of installation operations, including resource loading and financial accounting
- Develop Shipboard Installation Drawings (SIDs) with installation cost as a major consideration and that reduce post award time delays
- Improve quality and timeliness of Government Furnished Information (GFI) for installations
- Improve rack design to enable component replacement with a long term goal to implement standardized racks
- Reduce touch time on ships for software installations including application pre-loading and store-front delivery

MILESTONES

Improve program GFI to lower installation costs and delays in first time installs (CY2016)

Analyze and recommend rack approach for CANES Objective Baseline 2 and standardization of racks across SPAWAR (CY2016)

Develop installation efficiencies pilot to provide loading applications proof of concept in the CANES production facility vice onboard ship (CY2016)

MEASURES OF PERFORMANCE:

- Installation cost, compared to installation will and should cost, for major installations
- Measure install cost estimates on Ship Installation Drawings over time on similar installations as a measure of drawing cost to install
- Percentage of software pre-loaded
- Number and cost of design related liaison action requests with responsible parties identified

MEASURES OF EFFECTIVENESS:

- SPAWAR installations should improve in cost, schedule and quality
- CANES rack recommendations should improve install cost and schedule
- Number of applications pre-loaded in the lab
- Projected time saved loading applications on ship, based on lab effort (plan to measure actual in FY17)

Objective 1.C: Identify, Mature, Integrate, and Deliver Technical Capabilities

Technical capability insertion, encompass all types of advanced modernization, specifically targeting technologies that are evolving, emerging, and disruptive. Technical capability insertion activities are captured under four categories (identify, mature, integrate, and deliver) that form an "innovation pipeline". Specific activities are assigned to each category:

Identify: Map current, evolving, emerging, and disruptive technologies to identified needs (e.g., operational gaps, reductions in manpower and cost, increased effectiveness). Leverage technology surveys, Portfolio Health Assessments (PHAs), Integration & Interoperability (I&I) and N81 studies. Partner with Defense Innovation Unit-Experimental (DIUx). Define the process to communicate gaps.

Mature: Further develop technical capability, track Technology Readiness Level (TRL) transitions and use experimentation venues (formal and informal, e.g. Fleet Experimentation) to demonstrate military utility. Engage and coordinate with PORs.

Integrate: Transition technology to capability for POR (existing/new). Continue experimentation (e.g., in Enterprise Engineering and Certification (E2C)). Develop fielding plan and consider logistics tail.

Deliver: Increase current technology delivery levels with the goal to transition capability into standard fleet operations with training and logistics support.

The result of these activities is an organization that is better able to get the right technology to the warfighter at the right time.

MILESTONES

Identify 16 diverse candidate technologies that have gone through, or are currently in at least the first two stages of the innovation pipeline (CY2016)

Establish metrics (e.g., Technology Readiness Level, transitions, time, exit or disposition TRL, role of Technology Transition Agreement (TTA) experimentation venues) for the 16 candidate technologies (CY2016)

Complete and evaluate phase 3 of working prototype Science and Technology (S&T) database (CY2016)

Validate metrics, analyze pipeline flow (technology to capability to POM to POR to warfighter) and merge with developed S&T database for the 16 candidate technologies (CY2016)

MEASURES OF PERFORMANCE:

- Identify: architecture baseline complete; SSC work acceptance alignment; TTA tracking
- Mature: TRL velocity; formal measurement documents, TTAs managing technology expectation; number of successes demonstrating military utility
- Integrate: Products linked to baseline architecture; cost/schedule executes to plan
- Deliver: Successful percentage of TTAs; number of capabilities that reach desired end-state

MEASURES OF EFFECTIVENESS:

- Fleet experiences faster delivery of advanced technical capabilities
- Advanced technology is tied to what the fleet needs and wants
- Users perceive the value added of technology insertion

ENABLE MODERN INFORMATION TECHNOLOGY SERVICE DELIVERY

Delivery of modern information technology and services must consider the infrastructure (e.g., hardware, computing platform, transport layer) and applications while balancing the imperatives of affordability and "speed to market." This is inclusive of afloat, ashore and aloft segments of the battle space. It includes the applications we provide, those we host and systems connected to our networks that are developed by other organizations.

Objective 2.A: Provide Modern IT Infrastructure Services

SPAWAR and its affiliated PEOs have the responsibility to deliver IT solutions to users across the Department of Navy (DON), ashore and afloat, CONUS and OCONUS. This requires SPAWAR and affiliated PEOs to acquire, deliver, monitor, and sustain a modern IT infrastructure, which includes our computing devices, monitors, printers, data centers, networks, and even the software that resides on our servers and allows our systems and applications to run. In the very near future our IT infrastructure will also include cloud services from both government and commercial providers. This extensive IT infrastructure or "backbone" enables the enterprise's 964,000+ active military, reserves and civilian users to securely and efficiently transmit, retrieve, and store digital data on the DON's classified and unclassified networks every day.

Teams across PEO EIS, PEO C4I, SSC Atlantic, and SSC Pacific will be engaged in working on all aspects of Objective 2.A. Specific expertise will be drawn from all competencies across the SYSCOM.

MILESTONES

Continue consolidating DON networks and data centers, transition support of the Navy Enterprise Data Centers to the NGEN contract, and bring the OCONUS ONE-Net network up to NMCI standards. This "right-sizing" & standardization of our IT footprint is essential to reduce costs and secure all operations occurring in the cyber domain (CY2016)

Continue reducing the number of afloat network programs of record (e.g., ISNS, CENTRIXS, SubLAN, SCI Networks) through the continued fielding of CANES, to improve the Navy's cybersecurity posture and reduce the amount of end-of-life equipment in the fleet (CY2016)

Prepare DON networks and supporting infrastructure, to include completing build-out of the Navy's Cloud Access Point (CAP), for integration with commercial cloud environments

Migrate applications to commercial service providers' cloud environments, leveraging lessons learned during previous pilots (CY2016)

Document and manage the configuration of our extensive IT infrastructure, specifically the hardware and software (systems/applications) across our afloat and ashore IT environments; reducing variations in configuration, sustainment costs and cyber risk to the DON (CY2016)

Integrate industry trends into IT infrastructure capability roadmaps, so that we can increase the speed at which we deliver needed capability to the fleet and user community (CY2016)

Update computer operating systems (i.e. Win 7 to Win 10), install new/upgraded hardware ashore and afloat, and enable mobile device access (CY2016)

MEASURES OF PERFORMANCE:

- Operating system upgrade – progress / schedule metric
- Mobility infrastructure (i.e. Good Server, BES install/ upgrade) – progress / schedule metric
- Help desk service calls relative to infrastructure / operational performance
- Speed to capability for innovation cell enterprise challenges – schedule metric
- Cloud access point / infrastructure – completion/progress schedule metric

MEASURES OF EFFECTIVENESS:

- Operational exercise costs, or average cost per seat across the enterprise
- Unclassified (or classified via appropriate reporting venue) means of depicting cyber security outcomes (as a result of modernized infrastructure being in place)
- Operational availability of the NMCI, ONE-Net, and CANES networks
- Compliance with desired/approved configuration (hardware/software)

Objective 2.B: Provide Modern IT User Services

SPAWAR and its affiliated PEOs give our end-user community across the Navy the flexibility to choose and use the computing devices, systems/applications, and tools needed to execute their mission. The end-user services we provide include all aspects of IT ordering and delivery, for both hardware and software; enterprise-wide systems and tools; enterprise software licenses; digital storage, IT help desks, and cloud-based services. Our continual focus on expanding these services is aimed at improving the efficiency and effectiveness of the customer and driving down IT costs for the enterprise.

Our near-term efforts include bringing capabilities such as mobility, enterprise-wide email, single sign-on technology, analytics, and cloud-based software to every agency across the DON. As with Objective 2.A, teams across PEO EIS, PEO C4I, SSC Atlantic, and SSC Pacific will be engaged in working on all aspects of Objective 2.B. Specific expertise will be drawn from all competencies across the SYSCOM.

MILESTONES

Develop and deploy a Navy “App Store” with release of initial mobile apps (CY2016)

Transition systems/applications to cloud hosting environments; this includes performing cloud readiness assessments and preparing them for transition (CY2016)

Develop technical and compliance standards (architecture/data schema) for mobile and cloud-based system/application owners to “build to” (CY2016)

Assess capabilities of cloud-based enterprise productivity software (i.e. Office 365, SharePoint Enterprise)

Seek open architecture / open source solutions to reduce costs and dependency on vendor-proprietary solutions (CY2016)

Improve enterprise system and end-user service “user interfaces” to improve user experience, system interoperability, data integration, and data quality (CY2016 tactical and business system efforts will be identified as part of this objective) (CY2016)

Develop data analytics to support the DON MPT&E 21st Century Sailor and Marine and Sailor 2025 initiatives (CY2016)

MEASURES OF PERFORMANCE:

- Percent of cloud-ready apps and systems within Navy
- Help/service desk calls (relative to user services)
- Percentage of apps using automated patching
- Applications available in the Appstore
- User self-service of IT capabilities focused on depicting usage of “pull” versus traditional IT services “pushed” to users

MEASURES OF EFFECTIVENESS:

- Availability and usage of Navy Appstore (i.e. If the App-store is effective in helping the workforce do their job, then downloads and app usage should be high)
- Percent of Navy apps and systems by type of hosting/ provider environment (i.e. data center, cloud) and overall hosting costs
- Proportion of open architecture / open source solutions to vendor-proprietary solutions

OWN CYBER TECHNICAL LEADERSHIP

SPAWAR is the Information Technology and Information Assurance Technical Authority (IT/IA TA) for the Navy. We position the Navy to respond to the quickly changing cyber threat environment. We are the technical leader for interoperability and cybersecurity and establish the standards, tools and processes that provide the Navy a defensible cyber architecture.

We must also rapidly evolve tools, systems, and capabilities as new technology emerges to optimize cybersecurity and readiness across the Navy's enterprise. We will use established baselines, configuration management and an assessment of security posture to manage change supported by an agile cybersecurity certification process codifying our architecture, standards and risk processes.

Objective 3.A: Align Navy to a Common Technical Approach for Cybersecurity

SPAWAR as the Information Assurance (IA) Technical Authority (TA) and chairperson of the Information Technology (IT)/IA Technical Authority Board (TAB) will lead the Navy's Systems Commands (SYSCOMs) to a common technical approach for improving Navy cybersecurity. The following long term strategic goals are critical to meeting this objective:

Defense in Depth Functional Implementation Architecture (DFIA): Develop a common defense in depth cybersecurity architecture which will provide the technical backbone for delivering secure solutions for the future

DFIA Standards: Develop a common list of detailed requirements to ensure consistent implementation of DFIA across the Navy SYSCOMs

Risk Management Framework (RMF) Transition: Lead the Navy to a common RMF technical approach to assessing technical risk at the system level and ensuring the validator workforce is properly trained

System of System (SoS) Risk Assessment: Lead the Navy to a common technical approach assessing cyber technical risk at the SoS and platform levels

CYBERSAFE Technical Approach: Lead the Navy to a common CYBERSAFE technical approach to include the implementation and execution of CYBERSAFE and the identification and implementation of safeguards of critical components to ensure mission success in a cyber-contested environment

Cybersecurity Figure of Merit (CFOM): Provide a common technical approach to assessing the Navy's program of record (POR) ability to develop, procure, sustain and maintain a cyber-ready system (budgeting, acquisition, sustainment)

MILESTONES

Risk Management Framework (RMF) Transition
- Establish and conduct RMF validator training and initiate transition of SPAWAR systems to RMF (CY2016)
- Transition SPAWAR programs to RMF (CY2017)

CYBERSAFE Technical Approach
- Establish CYBERSAFE technical approach and establish and conduct CYBERSAFE training (CY2016)
- Initiate the CYBERSAFE assessment of SPAWAR systems (CY2016)
- Complete CYBERSAFE assessment of SPAWAR systems and conduct CYBERSAFE certifications (CY2017)

Cybersecurity Figure of Merit (CFOM)
- Define the CFOM process and identify and execute initial CFOM pilots (CY2016)
- Conduct CFOM evaluations for SPAWAR systems (CY2017)

MEASURES OF PERFORMANCE:

- Completion of scheduled DFIA and Standards
- Percentage of systems entering RMF
- Percentage of systems with CYBERSAFE Grade assessed
- Percentage of systems that have conducted a CFOM assessment

MEASURES OF EFFECTIVENESS:

- Percentage of PORs compliant with the DFIA & Standards
- Percentage of systems with RMF Authority to Operate (ATO)
- Percentage of systems with CYBERSAFE Certificate
- Percentage of programs that utilize CFOM to prioritize investments

Objective 3.B: Establish an Enduring SPAWAR Organizational Alignment to Own Cyber Technical Leadership

SPAWAR requires the integrated structures, communications, and resources to own cyber technical leadership for the Department of the Navy. The following strategic goals are critical to meeting this objective:

Structures: Create an organizational and leadership structure to manage oversight of SPAWAR's expansive and diverse cyber mission. The organizational and leadership structure will be responsible for the horizontal integration of SPAWAR cyber initiatives and activities across the Planning, Programming, Budgeting and Execution (PPBE) cycle. Integration areas include: internal and external communications, reporting, resourcing and tasking.

Communications: Annually publish the SPAWAR Cybersecurity Master Plan to provide overarching guidance to SPAWAR HQ, our supported PEOs, and the Systems Centers on the planning, execution and management of SPAWAR Cyber activities.

Establish and maintain a cyber war room which showcases SPAWAR's successes, current activities, and future initiatives to support positioning the Navy to respond to the quickly changing cyber threat environment. The war room will also be utilized as a classroom to train the acquisition work force on cyber requirements and a work space for teams to collaborate on communications, reporting, resourcing and tasking.

Resourcing: Submit integrated, consolidated and prioritized SPAWAR cyber Baseline Assessment Memorandum (BAM) and Program Objective Memorandum (POM) inputs to requirements and resource sponsors respectively. BAM requirement and POM Issue submittals will reflect the SPAWAR total enterprise requirement.

MILESTONES

Structures

- Charter and stand-up SPAWAR cybersecurity IPT (by 15 Apr 2016)

Communications

- Publish SPAWAR 2016 Cybersecurity Master Plan by 30 Apr 2016
- Draft SPAWAR 2016 Internal Communications Plan by 30 Apr 2016 and publish by 31 May 2016
- Draft SPAWAR 2016 External Communications and Stakeholder Engagement Plan by 30 Apr 2016 and publish by 31 May 2016
- Stand up Cyber War Room phase I by 15 Feb 2016

Resourcing

- Publish SPAWAR internal business rules and timelines for POM-19 Cyber Resiliency BAM and POM-19 Program Requirements Reviews by 30 Jun 2016
- Compile and prioritize the SPAWAR POM-19 Integrated Cyber Resiliency BAM requirements by 30 Sep 2016
- Compile and prioritize the SPAWAR POM-19 Integrated Cyber Resiliency Issues for submittal to Resource Sponsors by 15 Oct 2016

VISION: Rapidly Delivering Cyber Warfi

ACCELERATE AND STREAMLINE DELIVERY	ENABLE MODERN IT SERVICE DELIVERY	OWN CYE TECHNIC LEADERS
Increase Commonality in Deployed C4I Configurations	Provide Modern IT Infrastructure Services	Align Navy to a Technical Appr Cybersecu
Improve the Design for Installations and Decrease Installation Timelines & Cost		Establish an E SPAWAR Orga Alignment t Cyber Technical
Identify, Mature, Integrate, and Deliver Technical Capabilities	Provide Modern IT User Services	Certify and Deliv and Services t Sustainable Cyl Platform

PRINCIPLES: Relevant

SPAWAR Strategic Plan

Execution Year 2016

ghting Capabilities from Seabed to Space

BER
CAL
SHIP

REDUCE THE COST OF OPERATIONS

OPTIMIZE OUR ORGANIZATION AND WORKFORCE

END STATES

Common
roach for
urity

Enduring
nizational
o Own
Leadership

er Systems
o Enable
ber Ready
ms

Make the Best Use of Every Dollar

Optimize Lab Infrastructure at SPAWAR

Optimize Information for Effective Decision Making

Plan for Success: Reduce Rework and Optimize Resources

Forecast Demand and Optimize Workload

Manage Workforce Talent to Match Demand

STRATEGIC OBJECTIVES

Resilient

Responsive

MEASURES OF PERFORMANCE:

Structures
- Charter IPT that provides centralized oversight of SPAWAR cybersecurity efforts, including the horizontal integration of communications, reporting, resourcing and taskings

Communications
- Publish SPAWAR 2016 Cybersecurity Master Plan
- Publish SPAWAR 2016 Cybersecurity Internal Communications Plan
- Publish SPAWAR 2016 Cybersecurity External Communications & Stakeholder Engagement Plan
- Establish Cyber War Room

Resourcing
- Implement business rules and timelines for developing the SPAWAR POM-19 Integrated Cyber Resiliency Requirements (and associated issues) for submittal to the POM-19 Cyber Resiliency BAM and POM-19 Resource Sponsor Program Requirements Reviews

MEASURES OF EFFECTIVENESS:

Structures
- Clearly define roles, responsibilities, and accountability for cyber efforts across SPAWAR
- Integrate SPAWAR/PEO responses to cyber related tasking

Communications
- SPAWAR employees recognize their role and contribution to Navy's cybersecurity posture
- Integrate consistent cyber communications outside of SPAWAR
- Engage successfully with SPAWAR cyber stakeholders

Resourcing
- Integrate HQ/PEO/SSC requests for cyber resourcing to ensure the most critical cyber requirements are submitted to requirements and resource sponsors

Objective 3.C: Certify and Deliver Systems and Services to Enable Sustainable Cyber Ready Platforms

The execution of this strategic goal will provide the fleet and shore community with a documented, certified, and defendable cyber baseline supported by tools, training and maintenance standards. The end-state will greatly improve the ability of Navy platforms and shore activities to maintain a current cybersecurity vulnerability posture and provide the tools and skills necessary to maintain the documented cyber baseline. These first steps towards documenting and certifying the delivered cyber baselines will be effective in the measurement and improvement of SPAWAR's ability to comply with cyber directives such as Computer Tasking Orders (CTOs) and accelerated delivery of vulnerability patches to the fleet. These actions directly support the coordinated United States Fleet Forces Command (USFFC)/ Commander, Pacific Fleet (CPF) Aug 2015 message that cites attention to cyber hygiene is essential to creating and maintaining a culture of improved cybersecurity.

MILESTONES

Publish 1st Results: 2 months (Jan/Feb) with intent to be an enduring activity (CY2016)

Initiate USS Pinckney Pilot (Jan/Feb). Begin with impacting all ships coming out of avails (Mid CY2016)

Define a cyber certification pilot with criteria and process. Accomplish within existing C4I certification (CY2016)

Certify platforms and sites (CY2017)

Establish Fleet Commander Cyber Working Group and accompanying process and policy (Mid CY2016); Conduct a pilot and establish a repeatable process

Determine concept of operations and tactics, techniques and procedures for the ability to capture operational cyber baselines (CY2017)

MEASURES OF PERFORMANCE:

- Monthly brief to Local Configuration Control Board (LCCB) on delivery of cyber-compliant baselines
- Establish current WSUS/SAILOR implementation benchmark and measure to 100% compliance
- “Green” cyber dashboards based upon compliance with scan, patch and scan requirements and effectiveness
- Document certification process, establish the Concept of Operations (CONOPS), and conduct certification events
- Document and implement the cyber Departure from Specification (DFS) process
- Report on SPAWAR programs’ ability to comply with designated cyber directive tasking (CTO’s, IAV’s, etc.)

MEASURES OF EFFECTIVENESS:

- Deliver cyber-compliant baselines
- Accelerate SPAWAR delivery of vulnerability patches
- Reduce vulnerabilities in the operational environment
- Certify platforms and systems for cyber operations
- Measure number of cyber departures from specification granted and feed back to In Service Engineering Agent (ISEA) for awareness and management
- Measure SPAWAR cyber directive compliance (CTO, IAVs, etc.)

REDUCE THE COST OF OPERATIONS

We have a responsibility to our nation and our navy to make best use of every dollar to enhance warfighting capability. This means we must remain as efficient as possible in executing operations regardless of the fiscal environment. SPAWAR will increase efficiency by reducing costs through improvements to existing processes and procedures. Savings will be realized either directly or through cost avoidance.

Objective 4.A.1: Optimize Lab Infrastructure at SPAWAR

This objective intends to optimize lab infrastructure across the SPAWAR Enterprise, and constitutes one of two efforts under the broader SPAWAR strategic objective "Make the Best Use of Every Dollar." With representatives from the Systems Centers, the PEOs, and HQ, the objective will determine the appropriate footprint to support SPAWAR C4ISR programs of record (POR), including end-to-end testing capability.

Once realized, the objective will provide the SPAWAR enterprise with greater lab capacity aligned to POR requirements, and an increased capacity to test software installations up to the secret-level at a shore facility. This will enable SPAWAR to mitigate and correct issues, minimizing adverse impacts on fleet units, and ensure faster installation with a smaller personnel footprint.

An optimized lab infrastructure across SPAWAR will benefit the fleet by shortening the system development cycle; increasing the quality of the fielded systems and shortening pier-side system install time.

As a first step, the Systems Centers will conduct a survey to understand PEO lab requirements as they relate to their PORs. Data from this survey will help baseline the gap between current lab infrastructure and future PEO needs. Upon review of this analysis, the objective team will derive a list of prioritized investments, with the goal of starting facility modifications no later than FY18.

MILESTONES

Survey PMWs to understand the expected changes to their systems, and how those would change infrastructure needed to support them (CY2016)

Based on results of the survey, conduct gap analysis between required and existing lab infrastructure capacity (CY2016)

Develop and implement plan to close identified gaps. Facility modification would begin in FY17 (Program funds), and continue through FY18 (CIP funds) and beyond (MILCON funds) (CY2016)

MEASURES OF PERFORMANCE:

- Percentage complete on lab requirements baseline
- Percentage complete on lab infrastructure plan
- Percentage complete on plan to accommodate PEO EIS NGEN government lab
- Percentage complete on archibus implementation at SPAWAR HQ and SSC Pacific

MEASURES OF EFFECTIVENESS:

- Expand use of SSC Pacific Shared Development Environment (SDE)
- Expand use of SSC Atlantic Virtual Hosting Environment (VHE)
- Expand ability to increase level of software load (and potentially data migration) of PORs in SSC LANT/PAC labs vs. at the waterfront

Objective 4.A.2: Optimize Information for Effective Decision Making

The purpose of this objective is to make institutional data easy, accessible, reliable, consistent and secure to support informed planning and decision making by all. This requires transforming the organization's use, management and understanding of data. In order to optimize resource utilization, decision makers require information at their fingertips to influence organizational outcomes. Through employment of advanced data practices, master data management and exploitation of data analytics, the organization will shift from being reactive to proactive.

In CY2016, the echelon II business intelligence team will focus on migrating existing echelon II reports hosted in iRAPS (financial reports), development of initial echelon II workforce reports, maturing the information requirements definition of echelon II and establishing an operating model. The deployment and maturation of echelon II business intelligence capability will increase organizational effectiveness by creating "a single version of the truth" shifting from intuitive based decision-making to analytic-based decision making at the echelon II.

In CY2016, SPAWAR will formulate a data management program designed to make the best use and reuse of existing corporate data and business IT, as well as future SPAWAR business IT investment projects. Through successful implementation and maturation, we will eliminate the burden and costs associated with unnecessary data calls, data entry and uncoordinated Business IT initiatives and information silos while delivering exponential value.

MILESTONES

Define and establish echelon II business intelligence capability (CY2016)

Define and establish baseline enterprise information requirements (CY2016)

Develop data management organization construct, including methodology employed to support planned and emergent enterprise strategic intent requirements (e.g. governance, players, roles) (CY2016)

Define data management infrastructure (enterprise tools, data quality, data security and standards, etc.) (CY2016)

MEASURES OF PERFORMANCE:

- Migration of echelon II financial reports to SSC Atlantic business intelligence environment by Dec 2016
- Stand up echelon II business intelligence IPT capability by Jan 2016
- Delivery of build #1 echelon II workforce reports by Sep 2016

MEASURES OF EFFECTIVENESS:

- Identification of duplicative stand-alone data sources
- Identified efficiency (e.g. reduction in manual data manipulation, manual data calls)
- Support for enterprise information requirements via enterprise solution

Objective 4.B: Plan for Success: Reduce Rework and Optimize Resources

The scope of this effort will include the development of a SPAWAR scheduling instruction. The instruction will include a comprehensive set of tools, an implementation plan and improvements to processes used to plan and schedule the work of the command that allows visibility into and management of those plans and schedules. The intent is to make qualitative and quantitative improvements to planning and scheduling to allow management to have a better perspective of the use of their resources. As part of this objective, SPAWAR will formalize its processes and tools for consistently and comprehensively forecasting each requirement for a new or follow-on contract award. SPAWAR will establish and monitor the milestones for each prospective contract requirement, aligning resources (people and time) to meet the demand signal and anticipated award dates.

Ultimately, this objective will lead to the development of common Service Level Agreements (SLAs) to document performance agreements between the supported organizations - the PEOs - and supporting organizations - the Competencies and Systems Centers.

MILESTONES

Development and Use of Common Scheduling Tools and Practices

- Develop and brief the validation decision brief to leadership (Mar 2016)
- Develop SPAWAR instruction (Apr 2016 – Sep 2016)
- Implement approved management plan in phases (Sep 2016 -TBD)

Contract Planning as Test Case

- Confirm baseline of planned contracts for award in FY16 by Mar 2016
- Develop initial baseline of planned contracts for award in FY17 by Aug 2016; and a re-validated baseline by Dec 2016

Development of Common Service Level Agreements (SLAs)

- Develop a common SPAWAR SLA Template for consistent and streamlined documentation of commitments made between supported and supporting organizations (CY2016)
- Engage and deliver competency-based SLAs for FY17 business needs (CY2016)
- Based on SLA requirements & demand signal, each competency provide recommendation for changes (CY2017)

MEASURES OF PERFORMANCE:

Common Scheduling Tools and Practices

- Develop a SPAWAR scheduling instruction with a common method of scheduling with variations depending on program or project size
- Scheduling tool selection
- Centralize management and the use of a database to facilitate management decisions

Contract Planning as Test Case

- Update and issue, as applicable, existing SPAWAR / PEO guidance on project procurement strategy meetings
- Validate baseline of planned contract awards for FYs 2016 and 2017 using current tools
- Continue to improve early visibility into, and agreement on, milestone schedules for each fiscal year's contracts requirements

Common Service Level Agreements

- Establish common SLA templates and business rules in FY17
- Document and rationalize demand signals to assist management with alignment of resources to requirements
- Increase insight into customer demand signal which will help inform recommendations for changes in service delivery models – phased implementation

MEASURES OF EFFECTIVENESS:

Common Scheduling Tools and Practices

- Increase efficiency in procurement, production and installations through the use of schedules
- Increase cost savings through the effective and efficient use of the schedule to conduct risk analysis, qualitative improvements
- Improve resource allocations across programs based on accurate timeline reporting

Contract Planning as Test Case

- Balance the distribution of contract workload across the fiscal year; measured by comparing the award dates for new contracts made in FYs 2016 - 2018 to the awards in prior fiscal years
- Reduce the number of pop-up contract requirements; measured by comparing the number of planned contract awards to the actual number of contracts awarded

Common Service Level Agreements

- Clearly define roles, responsibilities, and accountability for funded efforts across SPAWAR
- Implement negotiations and agreements between supported and supporting organizations to ensure best value for required deliverables
- Document demand signal to help inform planning and resource requirements across SPAWAR

OPTIMIZE OUR ORGANIZATION AND WORKFORCE

SPAWAR will identify, validate and disseminate best-in-class practices, processes, methodologies, systems and technologies with the objective of improving the affordability and performance of cyber platforms and systems. SPAWAR's adoption of best-in-class practices will allow for rapid fielding of improved systems and equipment. In addition, implementation of best practice guidance can reduce the need for regulatory policy by helping to create a culture of continuous process improvement. Achieving this superiority compels us to excel in modern information related disciplines, and developing the workforce to execute this mission is the most essential ingredient.

Objective 5.A: Forecast Demand and Optimize Workload

Understand the staffing demand signal in sufficient detail to be able to forecast future total force workload staffing requirements. Be prepared to justify and defend these requirements via our OPNAV sponsors. Define and develop an annual systematic and repeatable process for establishing a future end-state workforce target.

Use this process to develop the end-state target for FY2019-2020. Pursue validation of the current workload requirement and baseline.

Near-term efforts will focus on civilian and military elements of total force and should describe the requirement in fairly broad terms. As a foundation, this team will pursue a set of general business rules for alignment of work among echelon II, echelon III, and the contractor support services (CSS) workforce.

In the mid-term, the level of detail used to describe the workforce demand will migrate from broad terms to detailed skills and experiences. In addition, the mid-term strategy is to incorporate the CSS elements of total force.

MILESTONES

Develop a systematic and repeatable annual staffing requirements generation process that is aligned to and supports DON POM events. Synchronize with the SSCs' A-11 process (CY2016)

Develop a repeatable methodology for collecting future expected workload

Develop business rules and initial execution process, articulating the data and parametric requirements to prepare for the enterprise workload planning conference (CY2016)

Develop and publish a SPAWAR Note announcing the enterprise workload planning conference. Convene Enterprise Workload planning conference; results to be used to support POM19 (CY2016)

MEASURES OF PERFORMANCE:

- Ensure end-state is developed, supported and endorsed by leadership after workload planning conference
- Distribute FY19/FY20 targets and define annual update process

MEASURES OF EFFECTIVENESS:

- Annual total force POM process is developed in draft, and distributed for comment
- FY19 total force workload demand is captured by organization
- POM 19 total force requirements are developed and defendable based on sum of requirements
- Total force demand will be understood in sufficient detail to allow leadership to make informed decisions on the allocation of the manpower supply
- An increase in leadership's ability to make informed decisions regarding billet reductions/realignments as related to prioritized workload

Objective 5.B: Manage Workforce Talent To Match Demand

SPAWAR talent management will focus on documenting the workforce current and future roles and assignments. Effective talent management will enable us to train and utilize a workforce with the right skills, identified to fill needed roles at the right time. Several of the following milestones are dependent on the pilot testing and potential selection of the NAVAIR Talent Management Dashboard as an enabling tool for managing our human capital across the enterprise. We will leverage the work done by PEO C4I and SSC Atlantic over the past two years to determine whether using the NAVAIR tool with some customization to meet our SPAWAR-specific business processes and organizational alignment supports proceeding with negotiations with NAVAIR.

MILESTONES

Pilot a process for talent management and workforce planning. Ensure pilot demonstrates/contains:

- Competency Development Models (CDMs) – roles, specialties, subspecialties, KSAs (CY2016)
- Employee population of tool with work experience, language skills, specialized military experience, degrees and certifications (CY2016)
- Business rules that include a mission funded approach as well as a Navy Working Capital Fund (CY2016) (CY2016) approach
- Business models for work roles, locations and sources for mission funded, Navy Working Capital Fund and contractor support services

Pilot an organizational assessment, reviewing strategy, challenges and opportunities (CY2016)

Conduct a talent review, identifying the readiness and potential for future assignments or positions as technology, environment and work changes (CY2017)

Conduct development planning, identifying relevant training and education programs, developmental assignments, and experiential opportunities (CY2017)

MEASURES OF PERFORMANCE:

- Track workload metrics: we will know gaps and hire to highest priorities
- Develop a talent pool of role experts and easily identify qualified members to fill, among many types of positions, DAWIA Key Leadership Positions (KLPs) and Critical Acquisition Positions (CAPs), subject matter experts, technical warrant holders
- Increase capacity to meet future demand
- Increase flexibility to develop new CDMs/KSAs as work demand or technology changes
- Increase proficiency in key roles and specialties over time

MEASURES OF EFFECTIVENESS:

- Obtain agreement on highest level roles of the community for the core CDM's at the tier 1 level (i.e., 5.0 tier 1 level engineer)
- Use the tool to track increases and decreases in the pool of candidates qualified for priority roles and assignments as reflected by data in the tool (example: IAMs, lead engineers, expert logisticians)
- Measure the adaptability of workforce talent to fill gaps, with the following specific measures:
  - Lower number of unfunded positions
  - Increase number of personnel able to fill multiple roles

SPAWAR Strategic Plan

Execution Year 2016

Summary

SPAWAR's Strategic Vision describes a journey of change and continuing development to provide the best support to the warfighter. SPAWAR's Strategic Plan and its detailed objectives, provide the measures and milestones we will focus on to remain on course to our Vision. Throughout the year, our operational drumbeat, reporting and communications will center on these foundational efforts. Each and every member of our SPAWAR team has either a direct or indirect role in achieving these objectives. As one team, we will move SPAWAR toward our vision to rapidly delivery cyber warfighting capability from seabed to space. Our efforts will contribute to a naval force that produces leaders and teams who learn and adapt to achieve maximum possible performance, and who achieve and maintain high standards to be ready for decisive operations and combat.

Targeted End-States Team Members

Team member names removed for public distribution.

ACRONYMS

AIT: Alteration Installation Team

BAM: Baseline Assessment Memorandum

BES: Budget Estimate Submission

BI: Business Intelligence

BMD TADIL: Ballistic Missile Defense Tactical digital information Link

BSO: Budget Submitting Office

CAP: Cloud Access Point; Critical Acquisition Positions

CDM: Competency Development Model

CFOM: Cybersecurity Figure of Merit

CIP: Capital Investment Program

COMPTUEX: Composite Training Unit Exercise

CPF: Commander, Pacific Fleet

CTO: Computer Tasking Order

CSI: Cyber Security Inspections

CSS: Contractor support services

DFIA: Depth Functional Implementation Architecture

DGSIT: Deploying Group System Integration Testing

DoN: Department of Navy

E2C: Enterprise Engineering and Certification

EMP: Event Management Plan

FCC: Fleet Cyber Command

FSET: Fleet Systems Engineering Team

GFI: Government Furnished Information

IAV: Information Assurance Vulnerability

I&I: Integration and Interoperability

INSURV: Inspection and Survey

IOC: Initial Operational Capability

IPT: Integrated Product Team

ISIC: Immediate Superior in Command

IMO: Installation Management Office

ISEAs: In-Service Engineering Agents

IT/IA TAB: Information Technology Information Assurance Technical Authority Board

KLP: Key Leadership Position

KSA: Knowledge, Skills and Abilities

LCCB: Local Configuration Control Board

MPT&E: Manpower, Personnel , Training & Education

MTJ: Multi-TADIL J

OSBP: Office of Small Business Programs

PAIE: Performing Activity Initial Estimate

PHA: Portfolio Health Assessment

PPBE: Planning Programming Budgeting and Execution

SM: Procurement Schedule Meetings

POR: Program of Record

POM: Program Objective Memorandum

PQS: Personnel Qualification Standards

PRR: Production Readiness Review

PTRB: Platform Technical Review Board

O-FRP: Optimized Fleet Response Plan

RMF: Risk Management Framework

SLA: Service Level Agreements

SDE: Shared Development Environment

SID: Shipboard Installation Drawings

SoS: System of System

STO: Systems Test Officer

TAB: Technical Authority Board

TRL: Technology Readiness Level

TTA: Technology Transition Agreement

USFFC: United States Fleet Forces Command

VHE: Virtual Hosting Environment

WSA: Work Shaping and Acceptance

Space and Naval Warfare Systems Command
4301 Pacific Highway
San Diego, CA 92110-3127
www.spawar.navy.mil