Space and Naval Warfare Systems Command

Strategic Plan

EXECUTION YEAR 2017

Rapidly Delivering Cyber Warfighting Capability From Seabed to Space

SPAWAR Strategic Plan
EXECUTION YEAR 2017

FOREWORD

This year marks the third execution year of SPAWAR Vision 2015–2022. This document is the executive summary of your efforts to further refine our strategy to best meet the requirements of the warfighter. We are extremely proud of the extensive progress our workforce has achieved. We are confident our organization remains on course to deliver the information warfare capabilities our Navy will need throughout the next decade and beyond. Our progress over the past two years has followed a measured and logical approach. This allowed us to make fundamental changes to our processes while still meeting the day to day requirements of the fleet warfighter. In our first year we established our long term vision and began evolving our strategic objectives to reach that vision. In 2016 we formalized discrete objectives to better align the enterprise to our vision. We have now developed and refined key processes, both internally and externally, to better address the unique challenges and opportunities of the information warfare domain. While substantial work remains, our progress indicates a fundamental shift for SPAWAR. Below is a partial list of accomplishments from 2016; take pride in your contributions to our mission, vision and support to the Navy warfighter.

2016 key accomplishments include:

ACCELERATE AND STREAMLINE DELIVERY

- PEO C4I instituted a C4I Baseline approach across all platforms in the PEO C4I domain. Completed C4I Baseline implementation activities including product roadmap system reviews, realignment of product fielding within budget to maximize C4I Target Baseline fielding, and conducted Multi-TADIL J train-the-trainer seminars in the three major fleet concentration areas
- Completed CANES rack analysis for improved design for ease of install; completed CANES Hyper-converged Infrastructure Pilot and initiated preloading applications in the CANES production facility to reduce installation timelines
- Implemented Installation Management Office alignment and teamed with planning yards to improve government furnished information quality
- Delivered Storefront 1.7 software as part of CANES SW 1.2, easing the software update process
- For candidate technologies (endeavors) in the innovation pipeline, identified key attributes and acceleration factors that drive successful transition into a program
- Completed rollout/evaluation phases 1–3 of prototype science and technology database

ENABLE MODERN IT SERVICE DELIVERY

- Navy interim cloud access point architecture established and operational
- Completed 46 CANES installs by end of year, providing the infrastructure for modern tactical afloat service delivery; 20 additional installs are in progress with another 14 in preproduction
- Consolidated 33 Navy data centers in 2016; currently providing hosting services to 300 systems and apps while leveraging nine CONUS hosting sites
- Migrated more than 1200 websites and four applications to commercial hosting; consolidated 32 apps to Navy data centers
- Significant progress on mobility solutions including NMCI mobile capability build-out to 34,500 user capacity; 29,500 users to date and adding Android devices; CONUS mobility solution in place with Blackberry shutdown complete; and Afloat Mobility Pilot successful in Trident Warrior 16
- Developed and established IT user services in areas of mobile apps, cloud transitions, standards and analytics including:
  - Established commercial cloud service offering; Cloud Store 2.0
  - Delivered 13 Manpower Training Personnel and Education mobile apps, and Afloat Storefront 1.7
  - Completed SPAWAR 5.0 Data Center Hosting Standard and Commercial Cloud Hosting Standard

OWN CYBER TECHNICAL LEADERSHIP

- Established initial framework for building cyber secure systems: 18 information assurance standards signed, the remainder are scheduled for development in FY17
- SPAWAR Cyber War Room established with classified (SECRET) collaboration and presentation capabilities
- Improved delivery of vulnerability patches; increased the percentage of systems using automated update services in Windows systems from 26 to 88 percent; provided one stop shop for systems requiring manual patching on SAILOR (increased from 24 to 92 percent)
- Completed 26 Operation Rolling Tide installations
- Completed three ship cyber baseline pilots focused on reducing vulnerabilities in the operational environment, with one in progress; results of pilots inserted into SURFOR Cyber Warfare Mission Area certification process
- Conducted 48 prioritized CYBERSAFE technical approach evaluations and foundational analysis of systems. Planned completion of evaluations is 2017
- Designated the Nuclear Command, Control and Communication - Navy (NC3-N) Chief Engineer (CHENG); coordinated across the Navy and DISA to synchronize NC3-N architecture development efforts, used a model-based systems engineering process to define the system-of-systems design and utilized a more consistent end-to-end test and integration methodology
- Implemented comprehensive design and architecture engineering technical authority across the entire C4I enterprise by our CHENG Directorate. This work builds from our superb performance as the NC3-N CHENG and Cybersecurity Information Technology/Information Assurance Technical Authority work and enables clear and consistent technical direction and implementation for all C4I systems-of-systems

REDUCE THE COST OF OPERATIONS

- Developed and implemented the ability to preload CANES SIPRNET software in Old Town to reduce installation timelines
- Completed lab infrastructure assessment to identify lab resource gaps and identify recommendations to address shortfalls
- SPAWAR Headquarters and SSC Pacific successfully using ARCHIBUS to improve facilities management
- SSCs expanded use of their respective Shared Development Environment and Virtual Hosting Environment
- Transitioned financial reporting capability into SPAWAR's business intelligence environment reducing the number of siloed business intelligence solutions
- Completed requirements definition for SPAWAR's business information demands
- Established SPAWAR's information governance to align investment decisions to business priorities to enable a data driven organization
- Established a baseline in April of 75 contracts to award in FY2016 (11 were added, 12 were canceled or placed on hold; of the balance of 74 actions, 56 were awarded within the fiscal year)
- Initiated transition from the Primavera scheduling software tool to Acquisition Milestone Tracker for use in FY2017

OPTIMIZE OUR ORGANIZATION AND WORKFORCE

- Implemented our capability-based in service engineering agent (CB-ISEA) organization; completed the consolidation of 58 equipment-based ISEAs into 16 capability-based ISEAs, substantially improving our ability to sustain end-to-end C4I capability to the fleet. This also improves our system design, testing and delivery processes
- Chartered Workload Identification and Requirements Team. Reviewed SSC Atlantic and Pacific workload acceptance processes and NAVAIR Workload Requirements and Planning tool
- Developed POM19 workload data collection process
- Identified key data elements and process steps from Echelon III acceptance process to form workload planning event, which validated demand and support POM19 manpower issues
- Implemented Talent Management Dashboard pilots to meet current and future demand

We have progressed from the planning and development stages of the SPAWAR Vision and can now fully focus on executing these processes across the Navy. We will deliver capabilities more efficiently. We will leverage modern IT services. We will provide the governance and standards to keep new and existing information warfare systems capable and secure. We will reduce costs and continue to develop our talented and capable workforce. This year we will build on your foundational work to rapidly deliver cyber warfighting capability from seabed to space. The warfighter, our Navy and our nation expect and deserve nothing less.

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

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

Achieving the SPAWAR Vision 2015 – 2022

VISION OVERVIEW

FOUNDATIONAL PRINCIPLES

RELEVANT

We assess our progress and adjust as required 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:

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.

ENABLE MODERN IT 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 battlespace. It includes the applications we provide, those we host and systems connected to our networks that are developed by other organizations.

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. We will use established baselines, configuration management and an assessment of security posture to manage change supported by an agile cybersecurity certification process to codify our architecture, standards and risk processes.

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.

OPTIMIZE OUR ORGANIZATION AND WORKFORCE

SPAWAR will identify, validate and disseminate best-in-class practices, processes, methodologies, systems and technologies to improve 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.

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 organizational vision. 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.

Accelerate and Streamline Delivery

Objective 1.A: Increase Commonality in Deployed C4I Configurations

Commonality in deployed C4I configurations delivers maximum warfighter capability and increased operational availability. When considering the entire C4I portfolio of products, no in-service ships share a single configuration baseline. Multiple new construction ships are designed and built with identical C4I suites; however, current acquisition and planning processes inject variance into these baselines as they are modernized. Over time, this objective will drive commonality in configuration baselines through coordinated approaches using: 1) System-of-systems (SoS) integration and engineering, 2) Alignment of funding to support integration needs, 3) Modifying PEO C4I processes for the delivery of end-to-end system baseline wholeness.

Success is achieved as PEO C4I defines C4I capability baselines for all classes of ships based on the class/platform mission requirements. This ensures the deployed operational capability matches the warfare requirement. C4I capability baselines will be maintained for groups of ships over multiple years in alignment with Optimized Fleet Response Plan (O-FRP) needs. Ultimately, the improved operational availability from common and familiar C4I configurations will directly impact the readiness of our warfighters.

MILESTONES

- PEO C4I, SPAWAR and the Fleet Readiness Directorate leadership engage with senior fleet and OPNAV leadership to garner advocacy for fielding and funding C4I baselines (November 2016 – April 2017)
- Seek N2/N6 sponsorship of C4I capstone requirements development process and funding the delivery of end-to-end system baseline wholeness; initiate consolidation of existing C4I system requirements (November 2016 – February 2017)
- Define and collect Baseline (B/L) 1.2 Element Artifacts: capability, engineering, cyber, test and human performance (e.g., training) artifacts (November 2016 – February 2017)
- Conduct Capability Baseline Review (CBR) – Initial (CBR-I), CBR-Design (CBR-D) and CBR-Readiness for B/L 1.2 (January – December 2017)
- Document test procedures for FY2017 Enterprise Engineering and Certification (E2C) test of B/L 1.2 (January – March 2017)
- Document data link personnel qualification standard fundamentals and systems; incorporate all watchstander position requirements for the totality of the data links portfolio (January – July 2017)
- Manage incorporation of test findings and setting/configuration modifications into future system installation and System Operational Verification Test / System Operational Test documentation (January – December 2017)

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 (SFP)
- Average percentage wholeness of platforms planned to receive a C4I Capability Baseline (as reflected in the SFP)
- Average percentage change in wholeness from SFP, Process Change Control Board (PCCB) Stage 3, PCCB Stage 2, to PCCB Stage 1
- Number of Operational Capability Build (OCB) derived test sequences tested prior to install
- Number of OCB derived test sequences tested post-install
- Number of OCB 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: Increase Quality of Installations and Decrease Installation Timelines and Cost

Our priority is to deliver premier C4I capabilities to the fleet as efficiently as possible. A key element in improving efficiency and reducing cost is designing systems and system technical refreshes with install cost and time as major considerations. Four main supporting efforts will help drive improvements into our C4I installations: 1) Move away from traditional "cut metal" upgrades toward delivering enhanced capabilities through in-rack replacements and software-only changes, 2) Producing better quality installation drawings, 3) Better integration of work into CNO availabilities, 4) Empower the installation workforce to control cost, schedule and quality.

By optimizing C4I installation processes, we can minimize "touch time" during high tempo ship availabilities and free resources for additional installations or other priorities. Our Sailors benefit by receiving the latest hardware and software capabilities faster and with less impact on operations.

MILESTONES

- Focus on improved program government furnished information, e.g. installation requirements drawing (IRD) and shipboard installation drawing (SID) (January – December 2017)
- Explore implementation of turnkey process for C4I modernization (January – December 2017)
- Implement will- and should-cost for major ship alterations (ongoing)
- Propose and incorporate installation duration key system attributes for future system designs and tech refreshes (ongoing)
- Incorporate lessons learned and rack improvements recommended from the CANES Hyper-converged Infrastructure Innovation Pilot (CHIIP) rack analysis (October 2016 – September 2017)
- Institutionalize the processes performed for the application pre-loading proof of concept ("APPLE PIE") to pre-load applications (November 2016 – August 2017)
- Leverage the afloat storefront efforts for pushing out application widgets and updates over the air (November 2016 – August 2017)
- Implement continuous development and integration concept of operations (November 2016 – August 2017)
- Leverage PMW 160 efforts to automate the CANES configuration and production efforts (November 2016 – August 2017)

MEASURES OF PERFORMANCE

- Installation actual cost compared to installation will- and should-cost for major installations
- Measure performing activity initial estimate (PAIE) install cost estimates on SIDs over time on similar installations as a measure of drawing cost to install
- Percentage of software preloaded; percentage of shipboard time saved
- The 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 preloaded in the production facility; metrics established for tracking the time saved on board ship
- Actual data of time saved loading applications in the production facility vice on board ship
- Decrease in manual steps/processes from development to production that lead to improved configuration management

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

Rapidly evolving information warfare technologies demand that we identify, recommend and implement improvements to quickly and effectively deliver these new technologies to the fleet. To implement this objective, we need to have awareness of current and future technologies, processes and infrastructure to assess the technology and reduce the barriers to transition. Specific efforts are captured under three activities: 1) Awareness of current and future technology, 2) Processes and infrastructure to assess technology, 3) Reduce barriers to transition.

Selection, coordination, demonstration and insertion of technologies will follow the guidance in the SPAWAR S&T CONOPS where applicable, and with identification of new approaches as required. The goal is to create functional technology insertion opportunities in all phases of acquisition and to minimize integration challenges. Technical solutions will come from the SPAWAR enterprise, commercial industry, academia, DoD enterprises and other R&D organizations. Success with this objective helps ensure our warfighters continue to dominate the battlespace with leading technologies.

MILESTONES

1: Awareness of current and future technology (2017):

- External technology assessment
- Request for information (RFI) topic to contracting office for action
- Release RFI
- Assessment of responses
- Evaluation of alignment to limited purpose cooperative research and development agreement initiatives
- Identify Technology Readiness Level (TRL) 5/6 technologies aligned with PEO gaps and enterprise architecture by mining internal S&T Analysis and Investment Reporting System (STAIRS) and external databases

2: Processes and infrastructure to assess technology (2017):

- Present targeted technologies to PEOs for assessment, investment and transition decisions
- STAIRS
- Prototype and experimentation
- Identify experimentation opportunities
- Situational awareness of experiments of SPAWAR interest
- Infrastructure assessment
- Infrastructure alignment to prototype demonstration and/or technical evaluation

3: Reduce barrier to transition (2017):

- Identify technology and insertion opportunities
- Identify windows of opportunity for technology insertion
- Describe acquisition on-ramp models

MEASURES OF PERFORMANCE

Milestone 1:

- Number of technologies forwarded to and reviewed by sponsors
- Progress toward RFI issuance and results analysis

Milestone 2:

- Technology development projects participating in prototype demonstration
- SPAWAR labs identified and disseminated for use in prototype demonstration

Milestone 3:

- Progress toward analysis of technology on-ramps and barriers (discussion, analysis and communication)

MEASURES OF EFFECTIVENESS

- Increase in technology identified, matured and transitioned to SPAWAR sponsors
- Increase in communication between Echelon III and PEOs on technology needs and potential technology solutions

Objective 1.D: Accelerate and Streamline Delivery of an Integrated C4ISR Baseline/Platform

Information warfare and C4ISR have different considerations compared to traditional defense acquisition programs. This objective focuses efforts to fundamentally change the way SPAWAR designs, develops and delivers these systems. It will define and implement an enterprise approach to engineering through a unified C4ISR capability as a software baseline (i.e. move to a software-defined C4ISR baseline) on a defined platform. It will feature standard tools and delivery mechanisms that provide the latest hardware, as well as support software that is not tightly-coupled to the hardware. It will also use the same tactical hardware and software baseline afloat and ashore. Key tenets include:

- Define and implement infrastructure and core services (e.g. well-defined Application Program Interfaces)
- Adoption of commercial best practices (engineering, software engineering and agile development, automated testing)
- Virtualization and insulation from operating systems updates
- Application rationalization and refactoring
- Delivery of new application software and updates over-the-air
- Move to a "fix, update and push" approach vice "scan and patch"

The goal is to achieve an environment that rapidly delivers new and updated C4ISR capabilities over-the-air, allows for the insertion of new technology and capability while maintaining backward compatibility, and is based on modern software engineering principles and practices. This effort will help maximize warfighter capability and increase operational availability of C4ISR systems.

MILESTONES

- Capture the overarching C4I requirement, (based on the integration of existing high level C4I program Capability Development Document level documents initiated in Objective 1.A) (September 2017)
- Define common architecture, which includes architecture, hardware/software infrastructure, core services and engineering processes (September 2017)

MEASURES OF PERFORMANCE

- Progress-to-Plan on creating an overarching C4I requirements document (reference Objective 1.A)
- Progress-to-Plan on defining common architecture

MEASURES OF EFFECTIVENESS

- Number of Platform Target Functional Baselines (for the Common Architecture) approved by the Architecture Governance Board (AGB)
- Number of standards and specifications (for the Common Architecture) approved by the AGB

Enable Modern Information Technology Service Delivery

Objective 2.A: Transform and Modernize Our IT Infrastructure

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 that SPAWAR and affiliated PEOs acquire, deliver, monitor and sustain a modern IT infrastructure, which includes the networking, computing and storage resources that allow our systems and applications to run. This extensive IT infrastructure enables the enterprise's active duty, reserve military and civilian personnel to securely and efficiently transmit, retrieve and store digital data on the DoN's classified and unclassified networks every day. Three overarching priorities are planned for 2017: 1) Improve ashore network services delivery, 2) Lead DoN Data Center Consolidation and modernization efforts, as chartered by ASN(RDA) and modernize our Navy's data centers, 3) Manage obsolescence, to include migrating to new operating systems while eradicating those nearing end-of-commercial support.

MILESTONES

Improving ashore network services delivery:

- Implement improved mission assurance capabilities to monitor and defend our networks. Initial capability (June 2017)
- Align PMW 205 IT service delivery requirements with the network transformation technical roadmap to assess and address gaps between user needs and infrastructure capabilities (March 2017)
- Develop an ashore Hybrid Network Topology that identifies how carrier/transport industry investments and existing infrastructure will be leveraged to improve service delivery, bandwidth, reliability and network resiliency (June 2017)
- Leverage existing NGEN technology refresh, modernization efforts and funding to initiate service delivery improvements (March 2017)

Continuing to consolidate and modernize our Navy's data centers:

- Reduce number of Navy data centers according to ASN(RDA)-directed and Navy Enterprise Information Governance Board (NEIGB)-approved FY2017 plan (September 2017)
- Develop a Navy private cloud. Cloud preparation assessment and concept for implementation (June 2017)

Managing obsolescence, to include migrating to new operating systems while eradicating those nearing end-of-commercial support:

- Migration to Windows 10 (WIN 10) across the enterprise (afloat and ashore). CANES SW2 Applications Integration System Integration Testing (June 2017)
- Mature processes to enable situational awareness and planning for all COTS components in the SPAWAR portfolio (April 2017)

MEASURES OF PERFORMANCE

Improving ashore network services delivery:

- Naval Network Transformation capability gap closure, Progress-to-Plan: projects planned, in execution, completed

Continuing to consolidate and modernize our Navy's data centers:

- Legacy data centers closed or transitioned to become Special Purpose Processing Nodes, Progress-to-Plan
- Navy private cloud Progress-to-Plan

Managing obsolescence:

- Number of platforms and applications converted to WIN 10 and number of WIN 10 installs, ashore and afloat
- Percentage of applications, per platform, converted to WIN 10 (accounting for those remaining with legacy, WIN 7)

MEASURES OF EFFECTIVENESS

- Real-time network awareness via common tool sets
- Increased service and network availability and reliability

Objective 2.B: Deliver Mobile Capability to the Workforce

The way we use, transmit and access data across the DoN is rapidly changing. Today, more than ever, our DoN workforce requires an increased level of connectivity and information availability at its fingertips, on any device and from any location. The ability to operate in a mobile workspace is pivotal to the DoN's ability to attract and retain the best talent. This ability is fundamental to executing the CNO, CMC and MCPON's "Ready, Relevant Learning and Sailor and Marine 2025" priorities. As the DoN's IT technical authority and IT service provider, SPAWAR and its affiliated PEOs will provide the mobile infrastructure, enterprise mobile applications and mobile standards that will enable the DoN to achieve its mobility vision. Two overarching priorities are planned for 2017: 1) Develop enterprise mobile application management (MAM)/mobile data management (MDM) solution(s), with the goal of converging to common enterprise-wide solutions in the future, 2) Expand the Navy mobile app environment.

MILESTONES

Develop enterprise MAM/MDM solution(s):

- Develop and implement an ashore MDM solution to be used CONUS and OCONUS (September 2017)
- Transition to Blackberry Enterprise Server (BES) 12.6 afloat (first install March 2017)
- Develop ashore/afloat mobile environment convergence plan, decision point brief (March 2017)
- MAM; inside and outside the container (September 2017)

Expand the Navy mobile app environment:

- Develop and deploy enterprise mobile applications (releases throughout 2017)
- Define enterprise mobile application development and release standards

MEASURES OF PERFORMANCE

Develop enterprise MAM/MDM solution(s):

- Number of additional users receiving mobile email capability
- Complete, resource convergence plan with decision points and capability introduction (Progress-to-Plan)

Expand the Navy mobile app environment:

- Performance metrics for SPAWAR-developed mobile apps (released, downloaded)
- Complete, resource application deployment plan with decision points and capability introduction
- Complete mobility standards (Progress-to-Plan)

MEASURES OF EFFECTIVENESS

Develop enterprise MAM/MDM Solution(s):

- Ability to edit documents within container
- Public Key Infrastructure-enabled web browsing via mobile devices
- Access to secure apps within container
- Access to apps with Navy information tailored to the individual outside the container

Expand the Navy mobile app environment

- User ratings of SPAWAR-developed apps
- User requests for additional apps and capabilities

Objective 2.C: Take the Navy to the Cloud

One of the most significant IT trends in the commercial sector has been the fundamental shift in how industry buys and delivers IT. Rather than investing in and supporting an extensive IT asset inventory, such as hardware, software and devices, cloud computing offers the DoN the ability to rapidly scale IT services to meet changing customer demand without the need to invest in and maintain costly hardware or physical data center facilities. As an augmentation to a small number of robust Navy enterprise data centers, commercial and government cloud solutions will transform how IT services are delivered to users across the enterprise. These cloud solutions will bring with them an expanded offering of network, cyber security and end-user productivity tools and will provide network service providers and application owners all of the benefits of cloud computing: on-demand self-service, rapid elasticity, the ability to pool resources in a pay-per-use environment and accessibility through standard Internet-enabled devices while adhering to the DoN's stringent cybersecurity standards. Three overarching priorities are planned for 2017: 1) Evaluate enterprise cloud productivity services for Navy implementation, 2) Continue to establish required government infrastructure to expand commercial cloud adoption, and 3) Transition existing systems and prepare new systems for cloud environments.

MILESTONES

Evaluate enterprise cloud productivity services for Navy implementation:

- Evaluate productivity and unified capabilities utilizing a hybrid architecture that supports on- and off-premises service delivery. Unified capabilities strategy approval (March 2017). Initial procurements (March 2017)
- Pilot capabilities of cloud-based enterprise productivity software. Productivity requirements included in the DoD Enterprise Services vehicle (December 2017)

Continue to establish required government infrastructure to expand commercial cloud adoption:

- Complete build-out and begin production operations of the enterprise cloud access point (June 2017)
- Develop system technical and compliance hosting standards (April 2017)
- Build out commercial hosting contract to support additional cloud service providers (April 2017)

Transition existing systems and prepare new systems for cloud environments:

- Transition our legacy systems and applications to cloud production environments. Provide hosting costs (January 2017). Initial virtualization status (February 2017)
- Establish cloud-based capability and environment that supports the development and deployment of future systems and applications (September 2017)

MEASURES OF PERFORMANCE

Evaluate enterprise cloud productivity services for Navy implementation:

- Number of users; systems/applications; and network, storage and computing resources migrated to the cloud
- Service delivery cost efficiencies gained via cloud migration

Continue to establish required government infrastructure to expand commercial cloud adoption:

- Publish cloud standards including reference Application Program Interfaces for Internet as a Service (IaaS)/Platform as a Service (PaaS)/Software as a Service (SaaS)
- Vendors added to commercial hosting contract

Transition existing systems and prepare new systems for cloud environments:

- Current state of each application by resource sponsor, identifying those that are cloud-ready (virtualized)
- Hosting options available for each cloud-ready application, to include cost projections for each environment
- Cloud-based development environment established, Progress-to-Plan for capability stand-up

MEASURES OF EFFECTIVENESS

Evaluate enterprise cloud productivity services for Navy implementation:

- Seamless service delivery between legacy and cloud-based environments
- Improved performance from legacy to cloud-based service delivery

Continue to establish required government infrastructure to expand commercial cloud adoption:

- Ability to assess cloud readiness for systems and apps for a Navy-approved, commercial cloud environment

Transition existing systems and prepare new systems for cloud environments:

- System and application owners will know the cost to host virtualized applications in the Navy's Enterprise Data Center and/or a commercial cloud environment
- System and app owners can redevelop their existing government off the shelf apps in a cloud environment

Vision: Rapidly Delivering Cyber Warfighting

Accelerate and Streamline Delivery	Enable Modern IT Service Delivery	Own Cy Techni Leader
Increase Commonality in Deployed C4I Configurations	Transform and Modernize Our IT Infrastructure	Identify: A Manageme Risk Asses
Increase Quality of Installations and Decrease Installation Timelines and Cost	Deliver Mobile Capability to the Workforce	Protect: Impro Hygiene, Develop and Target Arc
Efficiently Identify, Mature, Integrate and Deliver Technical Capabilities	Take the Navy to the Cloud	Detect: Situationa Continuous M Test and Cer
Accelerate and Streamline Delivery of an Integrated C4ISR Baseline/Platform	Plan for the Next Generation of Navy IT Services	Respond: to Incidents/Recove Capability Res
		Foundatio Organizational and Too

Principles:

Relevant ▪ Resilient ▪ Responsive

SPAWAR Strategic Plan

EXECUTION YEAR 2017

Capability from Seabed to Space

yber
ical
ship

sset
nt and
sment

ve Cyber
o Standards
chitecture

l Awareness,
onitoring,
tification

o Cyber
er to Ensure
storation

onal:
Alignment
ols

Reduce the Cost Of Operations

Optimize Our Organization and Workforce

END STATES

Make the Best Use of Every Dollar

Optimize Lab Infrastructure at SPAWAR

Optimize Information for Effective Decision Making

Forecast Demand and Optimize Workload

Manage Workforce Talent to Match Demand

Plan for Success: Support Services Contract Strategy

Make SPAWAR the Best Place to Work

STRATEGIC OBJECTIVES

Objective 2.D: Plan for the Next Generation of Navy IT Services

The Navy's operational environment is dynamic, especially in the cyber space where IT capabilities and vulnerabilities can rapidly change. The need to conduct cyber capabilities assessments, architecture refinement, configuration management, implementation planning, technical refresh, prototypes and pilots, and acquisitions – all in parallel – in this rapidly changing IT environment is our only constant. SPAWAR and its affiliated PEOs are experts in meeting the needs of today's warfighter while planning for the next generation of IT services that support every Sailor, Marine and civilian employee every day on the battlefield, on the flight deck, in the classroom and at the systems command. The capabilities being planned today will be critical to driving efficiencies across the DoN, making our workforce more productive and bringing greater data and information critical for tactical and operational decisions and mission planning. Three overarching priorities are planned for 2017: 1) Formalize and expand Innovation Cell framework, 2) Implement system of services, 3) NGEN Re-compete.

MILESTONES

Formalize and expand Innovation Cell framework:

- Completion of Innovation Cell Portal, collaboration, industry engagement and workflow capability (February 2017)
- Sign Innovation Cell charter (PEO authorization of roles and responsibilities) (January 2017)
- Execution of FY2016 and FY2017 Enterprise Challenges (September 2017)

Implement system of services:

- Agile Core Services (ACS) 2.1 common services deployment and sustainment aboard a designated ship (July 2017)
- ACS 3.0 tactical analytics stack maturations; software design drop in support of Distributed Common Ground System-Navy (DCGS-N) Increment 2 Fleet Capability Release 1 (February 2017)
- Implement PEO C4I system of services business plan; continuous development and integration CONOPS (March 2017)

NGEN Re-compete:

- This effort is critical to planning for the future ashore network and the delivery of IT services to the DoN. As Progress-to-Plan on the acquisition strategy is being reported in many senior level forums, we are highlighting it here for visibility within the 2017 Strategic Execution Guidance. We will continue to report progress via existing forums

MEASURES OF PERFORMANCE

Formalize and expand Innovation Cell framework:

- Number of registered users, companies and Enterprise Challenges responses in Innovation Cell portal
- Enterprise Challenge pilot capability assessments: multi-cloud tool to assess performance and possibly cost metrics across multiple cloud options, and location based services to perform device management within certain spaces

Implement system of services:

- Progress against fielding; application service adoption; application development onboarding into development operations environment

NGEN Re-compete (to be reported via existing forums):

- Re-compete schedule Progress-to-Plan, to include source selection evaluation board staffing

MEASURES OF EFFECTIVENESS

Formalize and expand Innovation Cell framework:

- Approved and established process for assessing technologies against refined requirements to quickly deliver capabilities to users

Implement system of services:

- Number of ACS services available to applications
- Published application hosting standards for ACS

NGEN Re-compete:

- Re-compete acquisition plans provide an effective and efficient means for service delivery and service offering to keep pace with customer demand, stakeholder interests, technology advancements and industry trends advancements and industry trends

Own Cyber Technical Leadership

Objective 3.A: Identify: Asset Management and Risk Assessment

To own cyber technical leadership, SPAWAR will develop common processes, standards and tools, as well as provide the fleet with known, defendable baselines. This objective draws on the first functional control group within the National Institute of Standards and Technology (NIST) framework to identify cybersecurity risk to organizational systems, assets, data and capabilities by developing institutional understanding.

SPAWAR will support this function through establishing and delivering documented cyber baselines, and through use of risk assessments and execution of a cybersecurity figure of merit (CFOM) to capture individual program risk. Understanding the structure and resources that support critical functions and the related cybersecurity risks enable an organization to focus its efforts and resources. Combining these efforts yields a deep understanding of cybersecurity risk and the development of robust supporting data that will inform budgeting, acquisition and sustainment decisions for platforms and programs of record. Leaders will have the data they need to resolve, mitigate or accept documented mission risks resulting from cybersecurity threats. The warfighter benefits as the Navy gains increased insight into mission risks today while applying this data to build in improved cybersecurity to our existing and future systems.

MILESTONES

Establish and Deliver Documented Cyber Baselines:

- Conduct Platform Configuration Control Board (PCCB) cyber reviews to enable early identification of system compliance gaps with key cyber directives. Ensure delivered systems support cyber hygiene requirements and deliver standardized program of record system and network configuration baselines
- Deliver cyber baseline documentation packages to designated AIRFOR/SURFOR platforms that capture key network/system configurations and settings, cyber compliance and system accreditation information to ship's force and TYCOMs for systems being modernized during CNO avails
- Implement a cyber deviation from specification (DFS) process that extends the existing fleet DFS process to enforce systems command approval of system and network changes during operations that may compromise the ship's cyber posture

Conduct Cyber Risk Assessments and CFOM:

- Conduct Cyber Risk Assessments: utilize the Tabletop Mission Cyber Risk Assessment (TMCRA) standard to determine mission-risk through a standardized assessment process. Discover and manage the nature and degree to which missions are vulnerable to cyber risk
- Analyze Navy networks, the vulnerabilities persistent on those networks, and identify the most likely attack vectors to assess risk at the system, system-of-systems and platform levels
- Risk management strategy: establish a risk based approach to improve cybersecurity by identifying the highest priority cyber risks to a designated mission and advising the appropriate managers of risk who either resolve, mitigate or accept the documented mission risks
- Execute CFOM: provide a common technical approach to assessing Navy's program of record ability to develop, procure, sustain and maintain a cyber-ready system (budgeting, acquisition and sustainment)
- Initiate and execute CFOM pilots in FY2017

MEASURES OF PERFORMANCE

- Measure ability to achieve Green Cyber PCCB criteria by A-9 "start of availability." Report PCCB results on a monthly basis at the joint PEO C4I/FRD installation readiness review board, recommend corrective actions and establish program specific improvement benchmarks
- Establish statistical trend analysis defining SPAWAR ability to support documentation delivery to SURFOR/AIRFOR platform requirements by program and by platform
- Cyber DFS: track number of programs with documented baselines that will support fleet policies and processes. Track via metrics the number of deviations granted and fed back to In Service Engineering Agent for awareness and management
- Number of systems that completed a cyber risk assessment and number of risks identified against correlating mitigations
- CFOM: percentage of programs that utilize CFOM and risk assessments to prioritize investments

MEASURES OF EFFECTIVENESS

- Delivery of cyber compliant baselines that support unit ability to manage and maintain key network configurations resulting in effective cyber hygiene regimen entering OFRP basic phase (delivery)
- In partnership with NAVIFOR and TYCOMs, assess the ability of units receiving cyber baseline to maintain "cyber green" status through OFRP work-up cycle and deployment (sustain)
- For units receiving a cyber baseline, NCDOC and units are able to achieve secure site mode by OFRP integrated/advanced phase (sustain)
- Cyber risk assessment reports are shown to be valuable in assisting programs to prioritize cybersecurity threats and vulnerabilities
- CFOM is demonstrated to assist programs to develop, procure, sustain and maintain a cyber-ready system

Objective 3.B: Protect: Improve Cyber Hygiene, Develop Standards and Target Architecture

Protecting our networks and systems from malicious activity provides the fleet unfettered access to all the capabilities of the information domain and the critical functions it supports. The NIST framework for managing cybersecurity risk highlights the protect function as developing and implementing the appropriate safeguards, prioritized through the organization's risk management process, to ensure delivery of critical infrastructure. Protecting the information domain requires attention from development of standards and architectures through operation and sustainment to ensure our systems are mission ready for the warfighter. The desired end state will greatly improve the ability of the fleet operators to achieve and maintain platform cybersecurity through delivery of the documentation, tools and training.

SPAWAR will support this function by leading the development of a system-of-systems (SoS) target architecture, Defense in Depth Functional Implementation Architecture (DFIA) and standards, and by improving fleet cyber hygiene through delivery of fully patched systems and operational monitoring.

MILESTONES

SoS target architectures:

- Through the Architecture Governance Board (AGB), lead the development of DFIA compliant, mission-based SoS target architectures across the SPAWAR enterprise

Improve fleet cyber hygiene through delivery of fully patched systems and operational monitoring:

- Minimize system vulnerabilities: refine system installation process to deliver fully patched systems prior to fleet turnover and accelerate patch delivery and distribution during operations
- Monitor fleet cyber posture: develop persistent systems and networks cyber monitoring, protection and configuration management capabilities through remote monitoring of deployed cyber tools (WSUS, VRAM and soon to be deployed auditing and system management tools)
- Align cyber security inspection (CSI). Work in partnership with stakeholders to recommend revision of existing CSI processes to support the evaluation of delivered cyber baseline artifacts and processes

DFIA and standards:

- Develop common DFIA and standards to provide the technical backbone for delivering secure solutions for the future

MEASURES OF PERFORMANCE

- Percentage of platforms and SPAWAR enclaves compliant with DFIA
- Percentage of completed standards available for program use
- Percentage of systems within defined enclaves, only connecting through approved control points
- Off-platform connections and boundary control points are known
- DFIA control points are known and approved
- Percentage of applications, local area networks and gateway devices is known
- Measure to a 100 percent standard, programs patched to zero site owned vulnerabilities at the end of modernization availabilities. Reduce number of POAMs required for systems not achieving threshold (targeted baseline ships only)
- Accelerate SPAWAR delivery of vulnerability patches: establish current WSUS/SAILOR implementation benchmark and measure to 100 percent compliance against the established DISA IAV(A)/ IAV(B) patch delivery requirements
- Percentage of ships able to maintain "green" vulnerability dashboards after delivery of cyber baselines to designated ships
- Percentage increase of CSI evaluation criteria that aligns to cyber baseline delivery criteria; measure against benchmark

MEASURES OF EFFECTIVENESS

- Completion, delivery and implementation of DFIA requirements and information assurance standards
- Development of SoS target architectures; cyber gap impact to mission is known
- Support maintenance of "green" cyber baselines; ship/site has zero site-owned vulnerabilities at end of availability or shore installation period for targeted units or sites
- Maintain "green" cyber hygiene: ship or site is able to manage vulnerability mitigation through work-ups and deployment within cyber compliance standards (IT/TA and CSI criteria informed though risk management framework implementation)
- In partnership with FCC/Office of Compliance and Assessments, support revisions to CSI 2.0 inspection criteria to evaluate the delivered cyber baseline

Objective 3.C: Detect: Situational Awareness, Continuous Monitoring, Test and Certification

The detect function within the NIST cybersecurity framework focuses on developing activities to identify an occurrence of a cybersecurity event. The function includes the categories of anomalies and events, security continuous monitoring and detection processes. Cybersecurity detection enables timely response and the potential to limit or contain the impact of potential cyber incidents to allow the platform(s) to keep fighting.

SPAWAR will accomplish the detection function through three lines of effort: 1) We will support tools to monitor and analyze the network to provide enterprise-level situational awareness, 2) Aligned with the risk management framework (RMF), processes will be defined for continuous monitoring to identify cybersecurity events and verify the effectiveness of protective measures, 3) We will test and certify cyber processes that will validate end-to-end cyber mission effectiveness. This includes CYBERSAFE certifications on the enclave and platform to validate that the appropriate safeguards have been implemented to ensure mission resiliency for the warfighter.

MILESTONES

Situational Awareness:

- Monitor and analyze the network to provide enterprise-level situational awareness (Sharkcage and Navy Cyber Situational Awareness (NCSA))

Continuous Monitoring:

- Define process for continuous monitoring to ensure the information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures (RMF Step 6)

Test and Certification:

- Identify and assess mission risk and/or shortfalls in cybersecurity between platforms and systems that interact to contribute to the accomplishment of a mission thread
- Develop the certification of cyber (Cyber Risk to Mission) process that validates cyber mission effectiveness
- Conduct CYBERSAFE certifications on the enclave and platform to validate the control points have implemented the appropriate safeguards for mission resiliency
- Develop SPAWAR certification policy to include rigorous cybersecurity criteria for PORs and non-PORs

MEASURES OF PERFORMANCE

- Percentage of identified networks tapped and mapped
- Continuous monitoring process defined and Information Assurance Technical Authority standard approved
- CYBERSAFE: percentage of systems with CYBERSAFE grade assessed
- Certify platforms and systems for cyber operations; SPAWAR owned components as a first objective
- Document a certification process, establish CONOPS and conduct certification events
- SPAWAR certification policy completed and signed (FY2017)

MEASURES OF EFFECTIVENESS

- POR systems have the ability to feed data for analysis in order to provide situational awareness for the DoD
- NCSA can consume data for use in DoD situational awareness
- Ability to tap and import network traffic for identified systems
- Standardization of network mapping tools and implementation into identified networks
- Continuous monitoring pilot demonstrates impact on active systems authorities to operate within the risk management framework process
- Fleet, FCC, TYCOMs and systems commands use common, agreed-upon criteria and monitoring/reporting tools to ensure networked systems and capabilities meet minimum cyber required standards to mitigate risk to the Department of Defense Information Network as defined by USCC/FCC directive
- Certification of cyber identifies gaps and overlays in existing certification processes
- Conduct certification of cyber mission thread risk assessment pilot on Nuclear Command, Control, and Communications (Q4FY2017)
- Improve cybersecurity posture and risk management of fielded systems within the SPAWAR/PEO C4I product suite through the certification process

Objective 3.D: Respond to Cyber Incidents/Recover to Ensure Capability Restoration

Just as the Navy trains for shipboard damage control to prepare for a kinetic attack, we must also prepare for a cyber intrusion that makes it through our defenses. Responding to cyber incidents and recovering critical operational effectiveness are the final functions of the NIST cybersecurity framework and shape our efforts for this objective. The response will include elements of planning, analysis, mitigation and improvements. Recovery activities will be developed and implemented to restore the capabilities or critical infrastructure services that were impaired through a cybersecurity event.

SPAWAR will focus on three key lines of effort to support response and recovery capabilities for the fleet: 1) The Cyber Incident Response Team will define proper processes and procedures to be maintained, then test ability to validate compliance, 2) The team will ensure activities are in place to prevent expansion of an event, mitigate its effects and eradicate the incident, 3) SPAWAR will also work closely with the fleet to define and develop cyber operating conditions that will enable fleet, group and unit commanders to mitigate adversary action and to maintain mission capability in a denied or degraded cyber environment.

MILESTONES

Cyber Incident Response Team

- Define response processes and procedures that will be maintained and tested to ensure timely response of detected cybersecurity events
- Ensure mitigation activities are in place to prevent expansion of an event, mitigate its effects and eradicate the incidents
- Stand up Incident Response Cell integrated into SPAWAR, IA/TA and FCC, C10F, NAVSEA, NAVAIR, NAVSUP, FFC processes
- Test our ability to validate agile reporting on elements that support cyber compliance from an operational perspective

Cyber Operational Conditions

- Define cyber incident recovery processes and procedures for the fleet to ensure timely restoration of systems or assets affected by cybersecurity events
- Work with the fleet to define and develop cyber operating conditions that will enable fleet, group and unit commanders to understand and execute cyber movement to mitigate adversary action and to maintain mission capability in a denied or degraded cyber environment

MEASURES OF PERFORMANCE

- SPAWAR is capable of forming a cyber-response in response to FCC/NNWC managed event
  - within 24 hours for a strategic/national network incident
  - within 48 hours for an operational/tactical network incident
  - within 96 hours for a non-tactical network incident
- SPAWAR Cyber War Room is materially ready to support incident response by Sept. 30, 2017. Initial tabletop cyber incident response exercise plan in collaboration with fellow systems commands is complete by Sept. 30, 2017, and provides vignette for annual SYSCOM cyber response cell exercise
- CYBERSAFE SECNAV instruction includes CYBERSAFE conditions
- Warfare certification incorporates criteria to grade systems and platforms capability to support cyber conditions
- Percentage of systems that have completed CYBERSAFE grade assessment

MEASURES OF EFFECTIVENESS

- SPAWAR cyber incident response cell has established policy and is ready for quarterly exercise by Oct. 31, 2017
- Fleet adopts unified framework of cyber conditions
- Manual procedures permit fleet to preemptively and reactively maneuver networks in response to network conditions

Objective 3.E: Foundational: Organizational Alignment and Tools

Providing cyber technical leadership for the Navy requires the development of a cybersecurity master plan outlining FY2018–2024 activities that will improve program and system delivery and improve the fleet's cybersecurity posture. SPAWAR must optimally align its organization and resources to meet the growing demands of cybersecurity across our Navy. We must develop and deliver cyber tools that will adhere to a documented acquisition, procurement and delivery roadmap to ensure we address capability gaps and support rapid deployment of cybersecurity tools and products to pace evolving cyber threats. This objective addresses these foundational requirements and should be an intrinsic part of our organization to achieve cyber technical leadership.

MILESTONES

Achieve Organizational Alignment:

- Develop, document and publish the SPAWAR FY2018–FY2024 Cybersecurity Master Plan to inform stakeholders of the depth, breadth and substance of budgeted and planned work to improve the Navy's operational cyber security posture (January – June 2017)
- Establish, document and publish the overarching integrated product team structure to manage the SPAWAR cyber program (January – June 2017)
- Draft and publish the SPAWAR cyber program CONOPS and instructions to manage the PPBE process to include acquisition, execution of work and deployment of information assurance capabilities (January – December 2017)

Tools Roadmap and Gap Analysis:

- Establish a cyber tool roadmap, create an agile environment to evaluate tools to address documented gaps and capture current and future budgeted tools destined for operational deployment
- Identify process, facilities and personnel requirements that will enable the enterprise to evaluate tools addressing near-term requirements and support experimentation, demonstration and concept evaluation
- Identify obstacles to the rapid deployment of cybersecurity products and tools

MEASURES OF PERFORMANCE

- Measure progress against the Jan. 1, 2017 baseline schedules defining the execution plans for the SPAWAR FY18–FY24 Cybersecurity Master Plan, the overarching IPT structure and the cyber program instructions
- Subjectively assess the improvement in SPAWAR/PEO's ability to defend the POM20 cyber requirements and issues
- Number of completed instructions compared to number of planned instructions
- Publish an annual analysis of SPAWAR cybersecurity tool capabilities to identify fielded, budgeted to field, or capability gaps
- Bi-annual analysis provided to Tools Sub-Working Group under IT/IA TAB Implementation Working Group, and aligned to SPAWAR's internal tools implementation processes

MEASURES OF EFFECTIVENESS

- All POM20 cyber requirements submitted via program requirements reviews to requirements and resource sponsors tie directly to the SPAWAR FY18–FY24 Cybersecurity Master Plan
- The overarching IPT structure provides increased ability for effective and efficient internal communications and engagement on issues that impose risk on successful execution of the SPAWAR FY18–FY24 Cybersecurity Master Plan
- Published SPAWAR cyber instructions reflect SPAWAR's ownership of cyber technical leadership for the Navy
- Repeatable process that supports the evaluation of cybersecurity tools is defined and utilized across the enterprise

Reduce the Cost of Operations

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

SPAWAR must optimize lab infrastructure across the enterprise to provide maximum benefit to the fleet. Existing infrastructure limits the number of systems that can be loaded and tested prior to installation, resulting in increased testing that must take place on the ship, delayed installation timelines and greater risk to those units. In addition, efforts to integrate applications and infrastructure early in the system development lifecycle are not readily supported by today's lab infrastructure. While working to ensure the lab infrastructure is available to meet these requirements, it is critical to make smart investments to meet program needs without unnecessary duplication of capability. By using virtual environments, consistent lifecycle processes and by making forecast data available for planning, an optimized lab environment will shorten the system development cycle, increase the quality of the fielded systems and shorten system install time. This objective will provide SPAWAR with a greater ability to effectively plan for and utilize lab capacity to meet cyber testing, fleet delivery and in-service requirements.

With representatives from the system centers, the PEOs and Headquarters, the objective is to determine the projected footprint to support SPAWAR C4ISR programs of record, including cybersecurity and end-to-end testing capabilities. During 2016, the systems centers conducted a survey to understand PEO lab requirements as they relate to their PORs. In 2017, data and insights from this survey will help baseline the gap between current lab infrastructure and future needs.

MILESTONES

- Combine the results of the 2016 lab needs survey with Echelon III understanding of technology and infrastructure needs to identify gaps in current lab capabilities/infrastructure (Q1FY2017)
- Develop and implement a plan to close identified gaps. Facility modification would begin in FY2017 (program funds) and continue through FY2018 (Capital Investment Program funds) and beyond
- Develop a lab requirements update strategy (FY2017)
- Develop a strategy, including resourcing, to develop and operate a sustainable and persistent operationally representative system-of-systems (SoS) test environment that can be connected with external Navy test capabilities (Q2–Q3FY2017)
- Demonstrate an operationally representative, SoS test environment to enable cyber assessment of Navy maritime networks in the systems centers labs (Q4FY2017)

MEASURES OF PERFORMANCE

- Percentage complete on lab infrastructure plan
- Number of classified and unclassified ship sets loaded prior to delivery
- Percentage complete on ARCHIBUS implementation at SPAWAR Headquarters, SSC Pacific and SSC Atlantic
- Number of baseline configurations that can be accommodated

MEASURES OF EFFECTIVENESS

- Reduced installation timeline
- Sustainable, persistent SoS end-to-end test strategy is developed
- Commander Operational Test and Evaluation Force operational test or certification of cyber test requirement is completed in a SPAWAR SoS test environment

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

This objective will make institutional data easy, accessible, reliable, consistent and secure to support informed planning and decision making. This requires transforming the organization's use, management and understanding of data. 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 2015, SPAWAR began this journey with COMSPAWAR's decision and investment to migrate Echelon II reporting into the future-state Enterprise Business Intelligence environment. In 2016, the Echelon II Business Intelligence team migrated existing Echelon II financial reports hosted in iRAPS (financial reports) into the SPAWAR Business Intelligence environment, reducing the number of siloed business intelligence solutions. SPAWAR established a Headquarters Business Intelligence capability and began working data foundation efforts for workforce, contracts and logistics. In 2016, SPAWAR began formalizing data management through an increased understanding and establishment of information governance.

In 2017, SPAWAR will continue to mature its business intelligence foundation and begin exploring additional analytical and visualization capabilities, live data connections with source systems driving increased synergy and alignment with other corporate activities. SPAWAR will further develop its information governance to align investment decisions to business priorities, including the instillment of data governance to increase the value and use of data to drive decision making.

MILESTONES

Deliver Enterprise Business Intelligence Reports - Workforce Management Report Build #2 (January – March 2017):

- Logistics report (SPIDER) build #1 (March 2017)
- Contracts report build #1 (March 2017)
- Quarterly builds per approved requirements (June – September 2017)

Develop Analytical Skills and Knowledge:

- Education training for data specialists (January – March 2017)
  - Define education and training requirement (January – March 2017)
  - Build training plan (April – May 2017)
- Execute approved training plan (June – September 2017)

Data Management Program Implementation:

- Formalize operational model for enterprise teams (June 2017)
- Develop and document key governance processes (September 2017)
- Enterprise resource optimization/shared resource model (April – June 2017)
- Issue formal SPAWAR policy (July 2017)

MEASURES OF PERFORMANCE

- Implement key governance business processes
- Deliver new reporting capability
- Deliver analytic training

MEASURES OF EFFECTIVENESS

- Future reduction identification of duplicative, stand-alone data sources and reports
- Identified efficiency and savings
- Number of analytic users

Objective 4.B: Plan for Success: Support Services Contract Strategy

SPAWAR must collaboratively establish and implement a strategy for support services that optimizes the capacity of the support services contractor workforce and balances the workload associated with planning, soliciting, executing and administering support service contracts. Through this strategy, SPAWAR will enhance competition and small business participation in the delivery of support services, ensure customer needs are met and solidify consistent best practices from planning through administration.

Support services covered under this strategy are generally those for knowledge-based, administrative and assistance services rather than niche or prime mission product/program of record services or project-specific services. Lessons learned through this strategy development effort and its implementation may inform future approaches and practices for planning, soliciting, executing and administering other service contract requirements.

MILESTONES

- Validate baseline of existing support services contracts (December 2016)
- Define "support services contracts" for the purpose of this effort (December 2016)
- Develop workload model/baseline of full time equivalent needed to administer or manage existing contracts and to award new contracts (February 2017)
- Conduct stakeholder analysis of requirements, best practices and constraints related to services contracts strategy (March 2017)
- Conduct industry engagement (May to November 2017)
- Assess other commands that have restructured their services contracting strategy (March 2017)
- Identify and take advantage of "quick wins" (December 2017)
- Develop, analyze and prepare courses of action for review (October 2017)
- Present courses of action to senior leaders (December 2017)

MEASURES OF PERFORMANCE

- Schedule
- Percent of deliverables completed

MEASURES OF EFFECTIVENESS

- Fully developed courses of action
- Creation of decision memorandum

Optimize Our Organization and Workforce

Objective 5.A: Forecast Demand and Optimize Workload

SPAWAR must understand staffing needs at all levels to forecast future workload and personnel requirements. Additionally, we must be able to explain and justify these workforce requirements to resource sponsors. As we continue to develop and refine the annual process, this objective directs that we repeat 2016 procedures that proved effective, prepare for 2018 staff milestones and priorities, and establish clear business rules that differentiate what work should properly be done by Echelon II billets versus what could be done by Echelon III or contracted support services. These three listed components (repeat, prepare, establish) will help develop the end-state workforce target for FY2020 and implement a staffing tool to support FY2021 and beyond.

Near-term efforts will focus on revising the current process based on lessons learned and begin to develop a high-level plan of action and milestones (POA&M) that shows what needs to be done to support timely tool implementation. By identifying high-priority implementation steps and barriers to implementation, the team can develop the near-term products that are necessary to support this long-term goal of workforce forecast.

MILESTONES

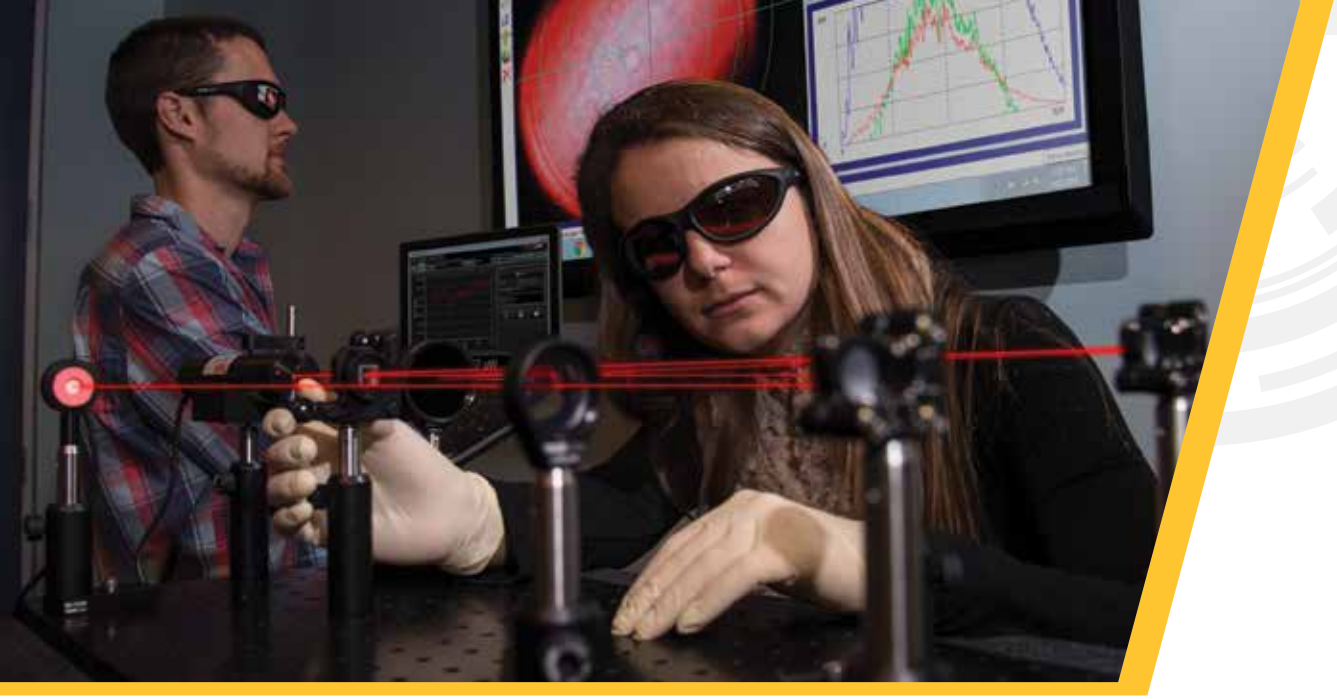
- Conduct POM19 analysis to identify trends with potential manpower impacts (November 2016 – June 2017)
- Continue to develop and refine a systematic, repeatable annual workload requirements generation process that is aligned to and supports DoN POM events. Identify new and increased work as well as work being reduced, realigned or discontinued that are potential offsets for new or increased work toward synchronization with the SSCs' A-11 process (January – July 2017)
- Once process updates are incorporated, repeat the 2016 process that resulted in a successful POM19 input, to include data collection, reporting and the workload demand and supply briefings (March – August 2017)
- Obtain approval and funding for a SPAWAR staffing tool. Develop a POA&M for the tool's implementation. Identify high priority needs and barriers. Develop the products necessary to support successful 2018 tool implementation (February – July 2017)
- Develop a model and/or business rules for Echelon II staffing. For program office staffing, use either the circa 2014 SPAWAR staffing model or a PEO consensus model based on programs/projects. Where a standard model cannot be applied, ensure business rules identify specifically why a position must be Echelon II (January – June 2017)
- Develop quantifiable risk assessment criteria for new or increased workload (January – June 2017)
- Develop and publish guidance for conducting the enterprise workload planning event (April/May 2017) Convene enterprise workload planning event. Results to be used to support POM20 (August 2017)

MEASURES OF PERFORMANCE

- End-state is developed, supported and endorsed by leadership after workload planning conference
- FY2019/FY2020 targets are distributed and annual update process is defined

MEASURES OF EFFECTIVENESS

- Annual total force POM process is developed in draft and distributed for comment
- FY2020 total force workload demand is captured by organization
- POM20 total force requirements are developed and defendable based on sum of requirements to include verification of internal reductions/realignments where available
- 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

The SPAWAR workforce must possess the necessary skillsets to meet the current and future requirements of our Navy. This objective will baseline our current workforce's skillsets and develop a process to identify, train and hire skilled individuals. To achieve this, we will determine the best use of Competency Development Models (CDM) to manage talent, including the possible use of an enterprise tool.

This objective will also support our current workforce with the necessary tools, education, training and experience to accomplish our mission, while we add new talent to help us stay on the leading edge for tomorrow. Throughout these efforts we will remain dedicated to equal employment opportunity, merit systems principles, and a diverse and inclusive workforce.

MILESTONES

- Review/validate/develop business rules for standard role names and nomenclatures across CDMs (January – March 2017)
- Develop process(es) to identify requirements for new/future workforce skill sets (January – December 2017)
- Determine the feasibility of a tool to identify/baseline workforce current skill sets, map to new requirements and identify those best suited for new skill set; develop requirements document and AOA of tools (January – December 2017)
- PEO/6.0 test/develop Talent Management Dashboard (TMD) to inform recommendation (April 2017)
- Develop SSC Atlantic TMD tool to inform recommendation of possible tool use (June 2017)
- If applicable, obtain approval and funding for a tool and develop a POA&M for the implementation of the tool
  - Identify high priority needs and barriers
  - Develop the products necessary to support successful 2018 tool implementation (July – December 2017)
- Use results of Objective 5A POM19 analysis to understand new and increased work requirements trends and to inform working groups as applicable (July – December 2017)

MEASURES OF PERFORMANCE

- Process for identifying new skills sets for future workforce developed
- Model/business rules developed for ensuring we are training current workforce with skill sets to meet future requirements and hiring individuals with potential to meet new/future requirements
- Feasibility of tool to identify/baseline current workforce identified with funding plan

MEASURES OF EFFECTIVENESS

- Future capabilities requirement process developed/approved
- Model/business rules for how we are going to train and hire for new/future skill sets approved.
- IT/tool recommendation coordinated with funding plan
- CDM guidance published
- Future skill set requirements will be understood in sufficient detail to allow leadership to make informed decisions on the hiring and training for future workforce. An increase in leadership's ability to make informed decisions regarding POM/Defense Acquisition Workforce Development Fund as related to training/education and hiring incentives for future workforce

Objective 5.C: Make SPAWAR the Best Place to Work

It is our foundational belief that SPAWARRIORs are our greatest strength. A motivated and satisfied workforce is absolutely essential to our mission success. In order to attract and retain world class employees, SPAWAR leadership is focused on making SPAWAR the best place to work. Through a combination of initiatives including work-life balance and wellness programs, more flexible work schedules and facilities improvements, our goal is to move SPAWAR into the top 100 best places to work among all federal agencies, and ultimately to become the best place to work.

Based on a sampling of more than 700 employees across SPAWAR as part of the 2016 Federal Employee Viewpoint Survey (FEVS), SPAWAR was ranked 134th out of approximately 300 federal agencies in terms of being the best place to work. SPAWAR leaders believe that being middle of the pack is not good enough – we can and will improve. We recognize that maintaining high levels of employee motivation and satisfaction are a critical dimension of workforce management and leadership. Successful achievement of Objective 5C represents leadership commitment to our workforce and making SPAWAR the best place to work.

MILESTONES

Survey employees and gather information:

- Compile SPAWAR survey responses (FEVS, Organizational Assessment Survey (OAS), Defense Equal Opportunity Management Institute Organizational Climate Survey (DEOCS)) and identify key trends (January – March 2017)
- Conduct face-to-face interviews with a sample population from each competency (January – March 2017)
- Administer FEVS survey across SPAWAR – ensure adequate publicity and encourage participation (April – June 2017)
- Conduct SPAWAR-specific surveys (ongoing)

Review current quality of work-life programs across SPAWAR and DoN and implement best practices:

- Gather information on SPAWAR and DoN best practices in work-life programs (e.g., telework, health and wellness programs, work schedules, facilities, exit/onboarding surveys) (January – March 2017)
- Brief recommended work-life program changes and additions (April 2017)
- Develop plan of action and milestones for implementation of approved recommendations/best practices (May 2017)
- Develop quality of work-life measures, including performance and effectiveness (June 2017)

Develop Improvement Plan:

- Using information from survey analysis and review of current efforts, develop improvement plans (ongoing)
- Based on OAS/DEOCS/FEVS results, develop questions for inclusion in future SPAWAR or competency-specific surveys (ongoing)

MEASURES OF PERFORMANCE

- Survey results (OAS, FEVS, DEOCS and exit surveys)
- Improvements in categories that influence work satisfaction and commitment; effective leadership, employee skills-mission match and work-life

MEASURES OF EFFECTIVENESS

- Marked improvement in employee satisfaction within each SPAWAR component and for the command overall
- Change leadership culture from top-down to bottom-up "Servant Leadership"

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