

# Strategic Vision

2015 - 2022



## 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.

## 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.

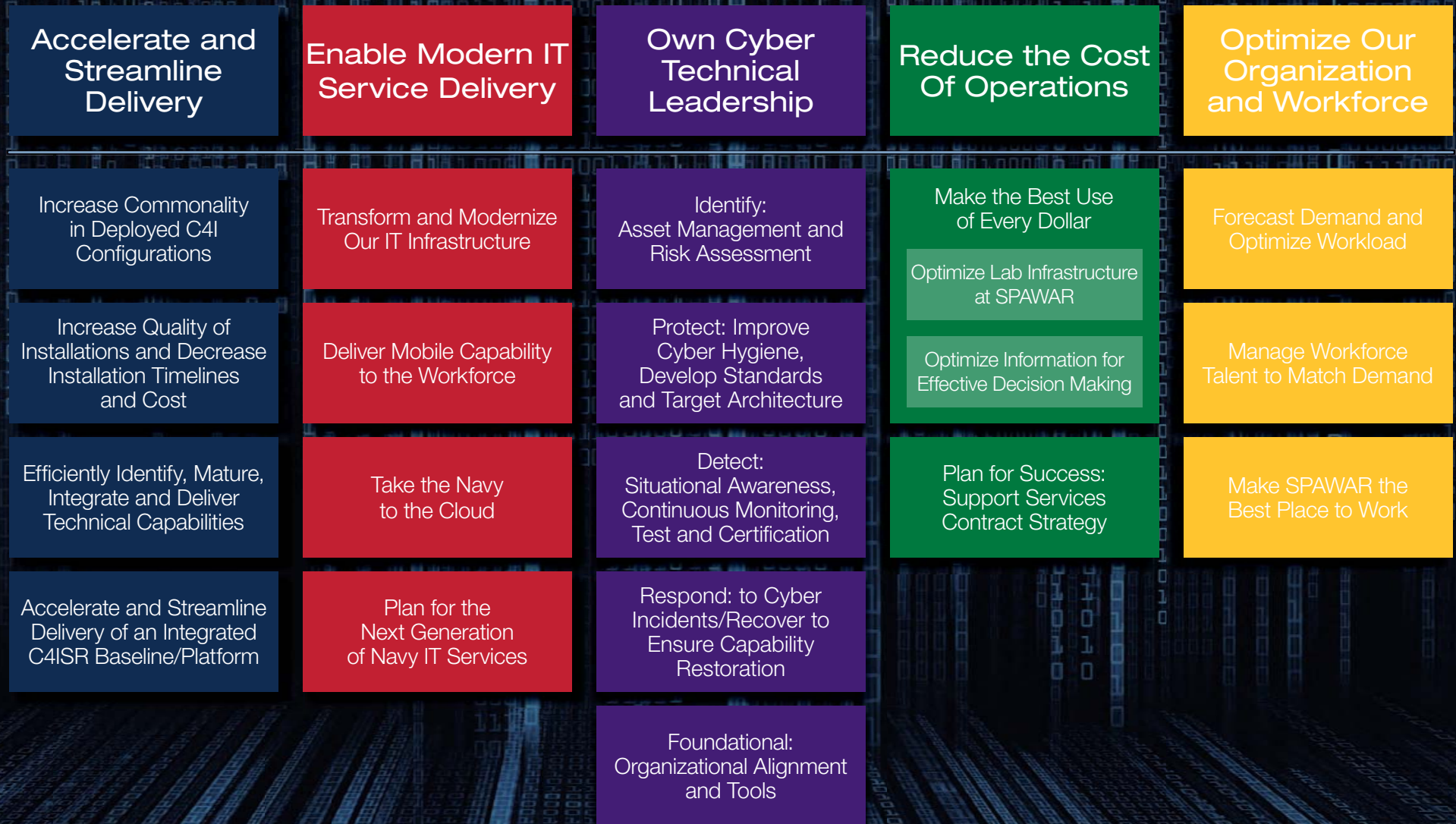
**VISION:** Rapidly Delivering Cyber Warfighting Capability from Seabed to Space



# SPAWAR Strategic Plan

## EXECUTION YEAR 2017

**Vision:** Rapidly Delivering Cyber Warfighting Capability from Seabed to Space



END STATES  
STRATEGIC OBJECTIVES

**Principles:** Relevant ■ Resilient ■ Responsive