



NSWCDD Technical Director - (540) 653-8103

Naval Surface Warfare Center, Naval Undersea Warfare Center

The Leaders in Warfare Systems Development and Integration

***Naval Sea Systems
Command
Cybersecurity Day***

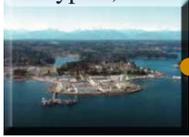
30 October 2015



Naval Warfare Center Enterprise

The NSWC operates the Navy's full spectrum research, development, test and evaluation, engineering, and fleet support centers for offensive and defensive systems associated with surface warfare and related areas of joint, homeland and national defense systems from the sea.

NUWC Keyport
Keyport, WA



NSWC Crane
Crane, IN



Naval Ship Systems
Engineering Station
Philadelphia, PA



NUWC Newport
Newport, RI



NSWC Headquarters
Washington, DC



NSWC Carderock
West Bethesda, MD



NSWC Indian Head
Indian Head, MD



EOD Technical Division
Indian Head, MD



NSWC Dahlgren
Dahlgren, VA



NSWC Panama City
Panama City, FL



Combat Direction Systems Activity
Dam Neck, VA

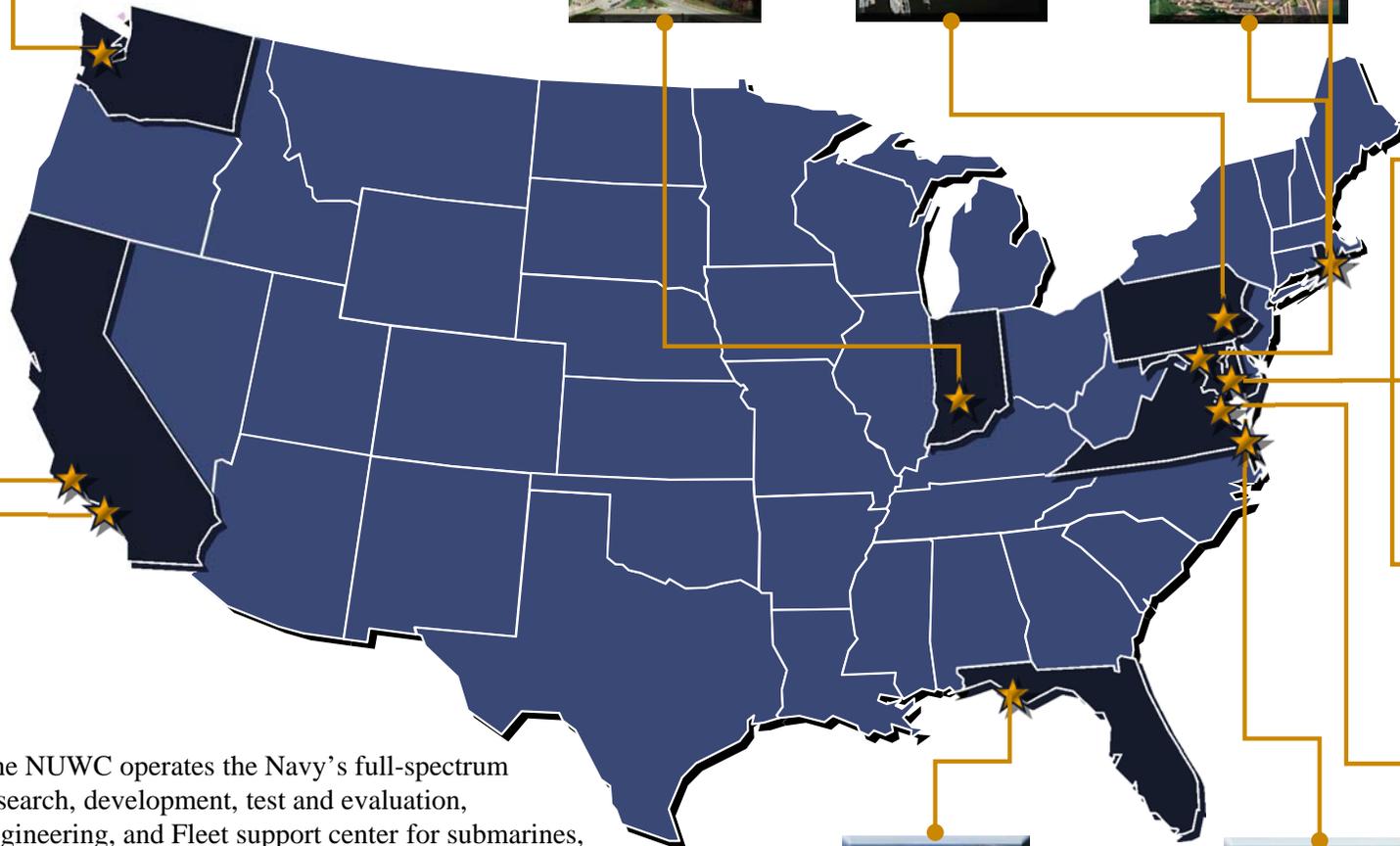
NSWC Port Hueneme
Port Hueneme, CA



NSWC Corona
Norco, CA



The NUWC operates the Navy's full-spectrum research, development, test and evaluation, engineering, and Fleet support center for submarines, autonomous underwater systems, and offensive and defensive weapon systems associated with USW and related areas of homeland security and national defense.





What We Do for the Program Offices/Fleet

Build an Affordable Future Fleet

Sustain the Current Fleet

S&T

R&D

T&E

Product Delivery

Fleet Support

Basic Research

Applied Research

Technical Risk Assessments

Sensor, System, & Missile Performance, Quality, Reliability, and Evaluation/Assessment

Element and Combat System Certification

National/Global Scientific Leadership

Rapid Prototyping

Environmental Testing

Tests @ Ranges/Major Facilities

Technology Refresh

Modeling and Simulation

Foreign Comparative Testing

Installs

Modernization & Alterations

Technology/Obsolescence Management

Patents

Human Systems Integration

Metrology & Test, Measurement & Diagnostic Equipment (TDME)

Analysis of Alternatives

Quantitative Fleet Feedback and Pre-Deployment Certification

Depot Maint Repairs

Cost-Performance Tradeoffs

Product Assembly

Systems Training

Onboard Tech Assists

Cyber Engineering

Integrated Logistics Support

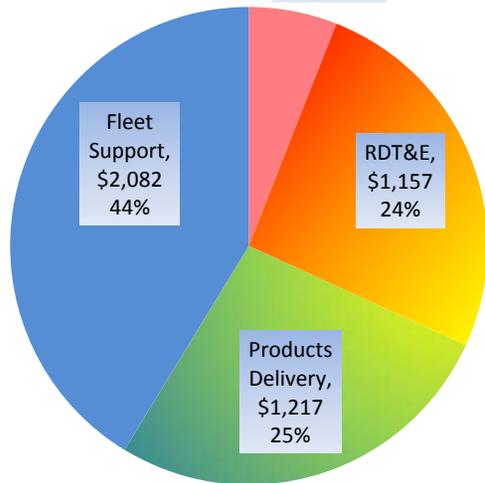
Distance Support

Information Assurance & Cyber Security

Integration and Interoperability

FY14 Reimbursable Funding (\$M)

S&T, \$314
7%

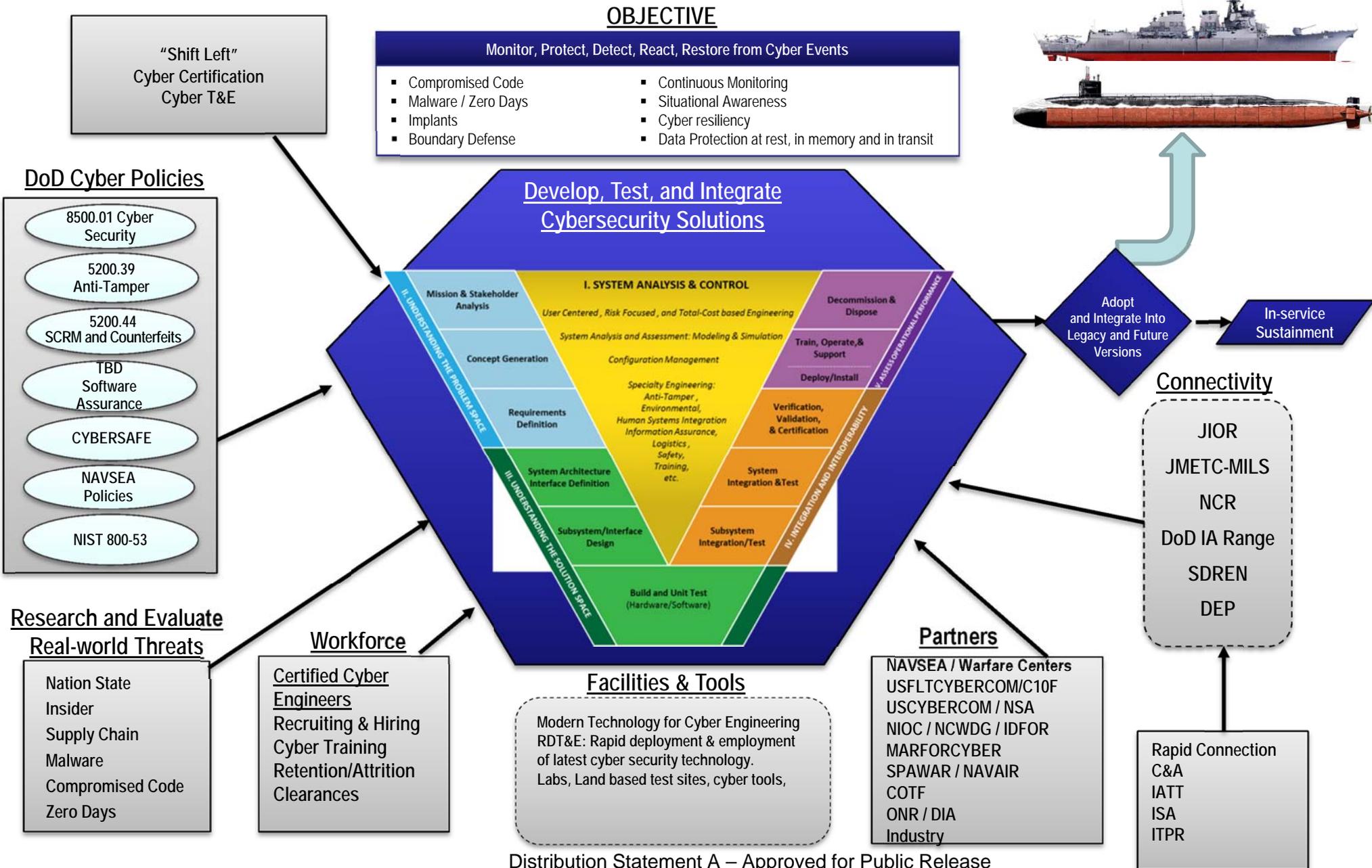
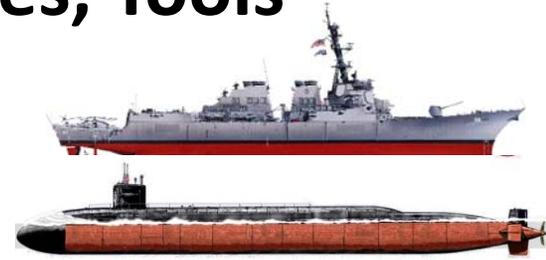


Providing technical expertise across multiple portfolios in multiple warfare areas.



Warfare Center Cyber Engineering

People, Processes, Facilities, Tools





NSWC / NUWC Cyber Security Priorities

- **Hull Mechanical & Electrical (HM&E):** Equipment is commercial-off-the-shelf - easily reverse engineered by an adversary, current HM&E architecture and equipment do not easily support built-in cybersecurity solutions, requires:
 - Scalable, composable, cyber-physical systems, resilience metrics, defense against insider threats, survivability of time critical systems, system / cyber state awareness, usable security
- **Navigation Systems:** Serve multiple enclaves and therefore difficult to separate into isolated enclave.
 - Presents cross boundary enclave security solution challenges.
- **Combat Systems Cyber Security:** Real time control systems with stringent latency requirements.
 - RDT&E community must develop and build combat systems that implement a defense in depth (DID) security architecture from the design phase.
- **Cybersecurity Threats:** Difficult to match known threat vectors to shipboard systems.
 - Published threats are typically focused on operating systems, software or hardware from enterprise IT systems.
- **Workforce Development:** To create an active/aggressive cyber security engineering workforce that plugs into ongoing cyber security engineering challenges and Risk Management Framework (RMF) initiatives
- **Prototyping:** Rapid deployment & employment of latest cyber security technology which includes tools, and infrastructure
- **Cyber Situational Awareness and Cyber Resiliency:** Combat, HM&E, & Navigation systems must:
 - Provide ability to notify commander when and if they were compromised
 - Identify when system is usable in full or degraded mode
 - Identify alternatives to aid the commander in completing the mission
 - Provide the ability to restore the system to a known, trusted state