



NAVSEA 04 Logistics, Maintenance and Industrial Operations

**Cybersecurity
Industry
Day**

October 2015

Introduction

1. **Name:** NAVSEA 04 Logistics Maintenance and Industrial Operations
2. **Area of Responsibility:** NAVSEA 04 is responsible for ensuring the proper construction, maintenance and modernization of Navy Ships.
3. **How it fits into the ‘Fourth Pillar’(Cybersecurity):** The SEA 04 Directorate is responsible for:
 - Supporting both NAVSEA and Fleet activities and assets
 - System operation and sustainment
 - System acquisition
 - Strategic information resource planning
 - Information Technology execution.
 - Cybersecurity

Where We Operate



The sun never sets on Navy Maintenance

- Naval Shipyards, Supervisor of Shipbuilding, Regional Maintenance Centers, Ship Repair Facility, Naval Submarine Support Facility and other industrial activities
- Over \$9.3 billion per year in ship maintenance supporting a workforce in excess of 51,000 military and civilians
- Oversight of 75 Information Systems and Networks

SEA 04 IT/Cybersecurity Priorities

- **Mobile Technology:** Development and deployment of mobile solutions (e.g. Electronic Technical Document (eTWD))
- **Virtual Operation Centers:** Sustain secure worldwide operations in support of consolidated data centers and enterprise applications
- **Training:** To create an active/aggressive cybersecurity workforce that plugs into Risk Management Framework (RMF) initiatives and ongoing cybersecurity challenges
- **Modern Technology:** Rapid deployment of latest technology supporting industrial operations
- **Industrial Equipment:** Integration of computer numeric control (CNC) industrial equipment in a connected environment

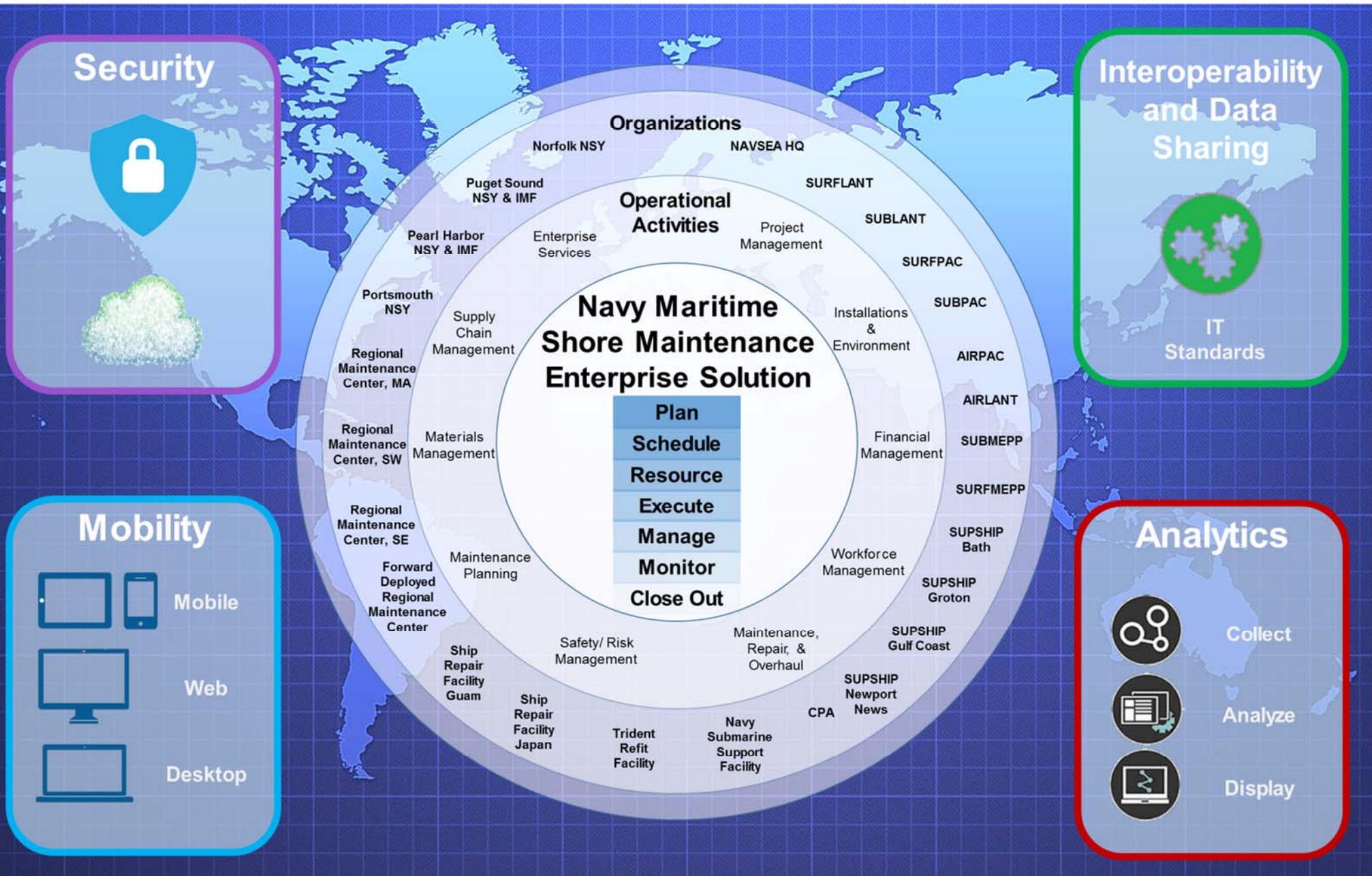
Cybersecurity Looking Ahead

- **Mobile Technology:** Provide Standard Operating Procedures/Processes that address the efficient and effective implementation of Mobile technology as it relates to a mobile workforce while ensuring a strong security posture for the Department of Defense Information Technology Networks. To include Laptops, Smart Phones, Tablets, Hand Held Devices, Wi-Fi, etc.
- **New Technology:**
 - Provide new or existing technology to support two factor authentication that improves upon or replaces the use of Hard Tokens such as CAC
 - Provide the technology to ensure PKE/PKI compliance can be enforced on all GOTS/COTS hardware and Software products (Examples: CISCO devices and Maximo)
- **Configuration Control Management:** Provide centralized control for information systems and industrial equipment
- **Knowledge Sharing:** Provide method of sharing cybersecurity issues/information across federal agencies

Seeking Industry Support

- **Reliable Cybersecurity Tools:** Provide reliable and cyber secure products that are easy to implement and sustain with respect to securing Data at Rest and Data in Transit.
 - Encryption for mobile devices / end users
 - Protected wireless environments
 - Rapid hardening of servers
 - Software patch management to reduce cost
 - Data encryption
 - Configured control support for industrial plant equipment/ update operating systems
 - Cybersecurity simulation and modernization tool set for cybersecurity workforce (CSWF) training and experience
- **Consolidated Cybersecurity Requirements:** Provide the ability to access a repository of approved remediation/mitigation strategies for vulnerabilities across the enterprise identified by STIG's, CTO's, ACAS and SCAP scans, IAVM's, etc.

Overview of SEA 04 IT AOR





SEA 04 Cybersecurity POCs

Director, Information Management Resource Division - (202) 781-2841

SEA 04 Ship Maintenance PMO-IT - (202) 781-1085