Cyber Security Industry Day
PEO Submarines

Agenda

- Product Lines and Organization
- Warfare Center Support
- Cybersecurity Approach and Strategy
- Challenges
- Cybersecurity Road Map
- Further Discussions – Team Submarines Representatives

Team Subs Cybersecurity
Product Lines and Organization

- Submarines
  - 688/688I Class
  - SEAWOLF Class
  - SSGN (OHIO) Class
  - SSBN (OHIO) Class
  - VIRGINIA Class
  - OHIO Replacement (OR) Class
- Trainers
  - Ship Control
  - Submarine Multi-Mission Team Trainer (SMMTT)

- Supported SHAPMs and PARMs
  - PMS-392
  - PMS-394
  - PMS-397
  - PMS-401
  - PMS-415
  - PMS-425
  - PMS-435
  - PMS-450
  - PMS-485
  - SEA-07
  - SEA-07TR

Warfare Center Support

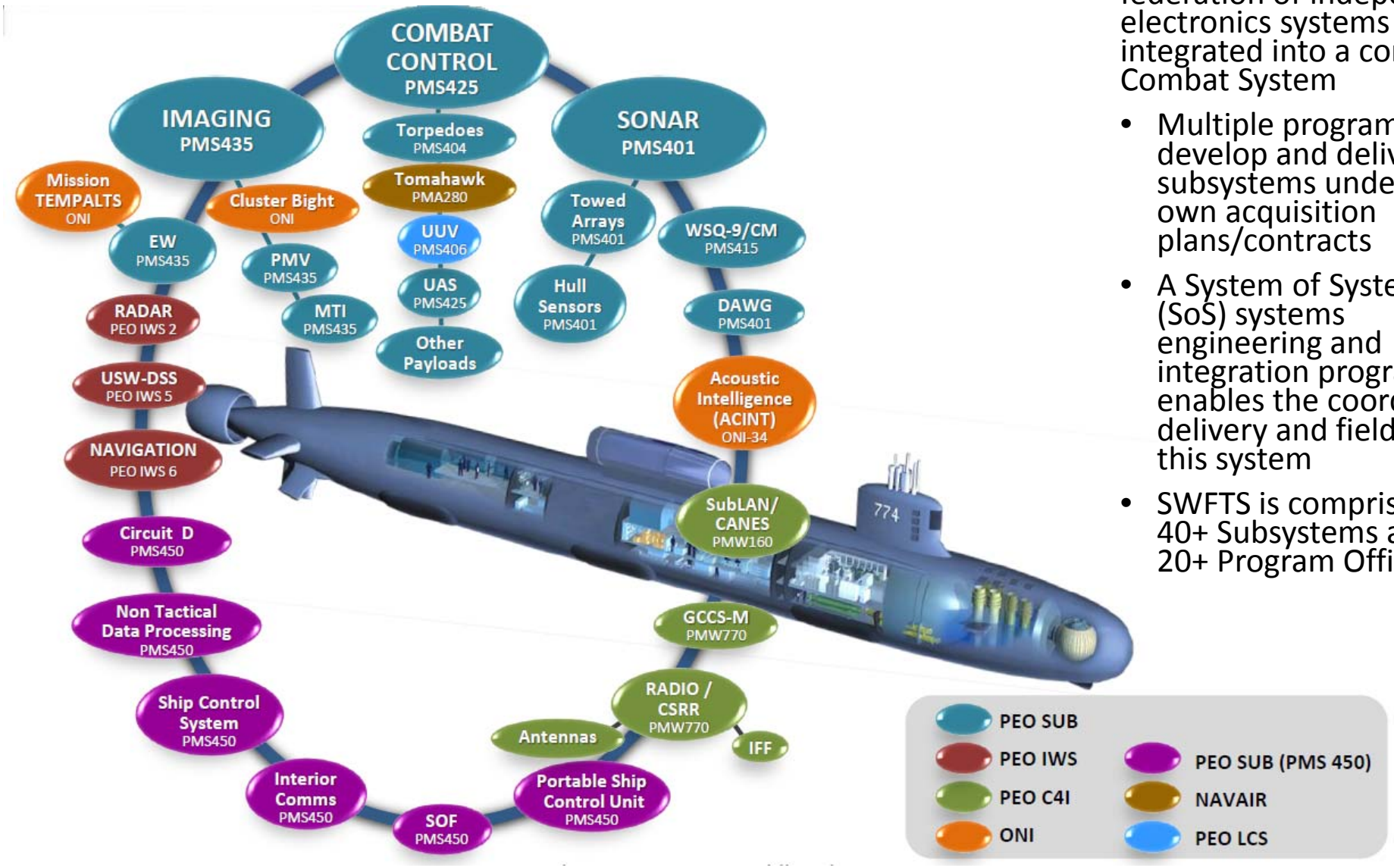
- Naval Undersea Warfare Center
  - Newport, Rhode Island
  - Cybersecurity In-Service Engineering
  - AN/BYG-1 TDA
  - Ohio Replacement Cybersecurity Engineering
  - Posture Transition Lead
  - Strike Warfare Cybersecurity
- Naval Undersea Warfare Center
  - Keyport, Washington
  - Accreditation Support
  - Security Engineering
  - IAVA/VRAM Management

Cyber Security Approach and Strategy

- Types of Systems
  - The entire realm
    - General Purpose Automated Information Systems (AIS)
      - SUBLAN/CANES - PEO C4I & Space
    - C4I – Common Sub Radio Room (CSRR) - PEO C4I & Space
    - Control Systems/Platform Information Technology (PIT) – Combat Systems
      - SWFTS/NPES – NAVSEA
      - Ship Control – NAVSEA
      - Others
    - Hull, Mechanical & Electrical (HM&E) – NAVSEA
      - IP based HM&E systems more prevalent on newer classes of submarines
        - VIRGINIA
        - OHIO Replacement (OR)
    - Trainers on the shore side - NAVSEA
      - All types of systems

Submarine Warfare Federated Tactical System (SWFTS)

Programmatic Federation



PEO SUB delivers a federation of independent electronics systems integrated into a common Combat System

- Multiple program offices develop and deliver subsystems under their own acquisition plans/contracts
- A System of Systems (SoS) systems engineering and integration program enables the coordinated delivery and fielding of this system
- SWFTS is comprised of 40+ Subsystems across 20+ Program Offices.

Cyber Security Approach and Strategy

- 8 years experience integrating Cybersecurity into submarine networks via Technology Insertion (TI) and Advanced Processor Builds (APB)
  - Subsequent to Combat Systems IA Compliance Mandates (2006-2007)
  - VIRGINIA TI-02 Non Propulsion Electronics System (NPES) Tactical Network
  - 688/688I TI-04 Submarine Warfare Federated Tactical System (SWFTS)
  - Bolted on Cybersecurity Solutions and CONOPS
- Submarine architecture approach unique in three ways
  - Space limitations drove the need for integrated systems
  - Space limitations drove the need to operate integrated systems at different security classifications
    - IA Rule Sets for different missions/security postures
  - Data Protection and segregation of data at different security classifications combined with the need to communicate with other networks of different security classifications

Unique Cybersecurity architecture approach provides the framework for a Defense In Depth Architecture

Cyber Security Approach and Strategy

- Team Subs Cybersecurity Initiatives
  - OHIO Replacement Platform Tabletop Mission Cyber Risk Assessment (TMCRA)
  - Accreditation process management improvements
  - Cross Domain Solution improvements
  - Virtualization of Enclave Guard
  - Integrated Cybersecurity into the Systems Engineering “V”
  - Integration of CYBERSAFE methodologies
  - SWFTS Vulnerability Assessment

SWFTS Vulnerability Assessment

- PEO SUBS teamed with Industry to put together a 3 phased SWFTS Vulnerability Assessment approach
  - Funded for FY-16
  - Phase I: G2 OPS
    - Network Topology/Architecture/PPS drawings
  - Phase IIA: GD MS/GD Fidelis
    - Cyber Test Bed – Threat/vulnerability analysis
  - Phase IIB: Raytheon
    - Threat/vulnerability analysis
    - Red Team Penetration Test
  - Phase III: MIKEL INC
    - Report analysis and scorecard
    - Metrics/Development Decision Aids
    - Statistically manage Cybersecurity Risk

Vulnerability Assessment forms the basis for development decisions and prioritization and drives updates to the Cybersecurity Strategy and Road Map.

CYBER SECURITY END-TO-END EVALUATION

NUWCDIVNPT Campus Network Supports Vulnerability Insight & Certification in Development of Secure & Resilient Submarine Systems & Architecture

Cybersecurity Challenges

- Accreditation for Platform Information Technology (PIT) and Cross Domain Solutions
  - Processes are long, cumbersome and geared toward General Purpose, Business Systems and Automated Information Systems
    - Vice special purpose Control Systems, Combat Systems, National Security Systems
    - Control System AO delegation to NAVSEA would help streamline the accreditation process
- Account Management/Access Control
  - Numerous passwords on SWFTS Network
  - Solution that works in a submarine environment
    - Single Sign On?
    - Biometrics?
- Supply Chain Management
- Secure Software Coding
- Fiscally Constrained
  - Implementation of Task Force Cyber Awakening (TFCA)/CYBERSAFE Initiatives
    - Require funding from external sources to execute

Team Subs Cybersecurity Strategic Road Map

*Threat Assessments/
RMF Continuous Monitoring

2015 | 2016 | 2017 | 2018 | 2019 | 2020 | 2021 | 2022

Vulnerability Assessment *

Vulnerability Assessment *

Vulnerability Assessment *

TI 14/APB13

TI 14/APB15

TI 16/APB15

TI 16/APB17

TI 18/APB17

TI 18/APB19

TI 20/APB19

TI 20/APB21

OR Tabletop Assessment ***

Enclave Guard
Secure Virtualization

**

TFCA/Cybersafe Implementation

**Account Management/ Access Control Solution

Cybersafe Control Point Hardening

Cybersafe TTP

Cybersafe Back Fit Plan

***Statistically Manage Cybersecurity Risk

Supply Chain Management?

Secure Software Coding?

Further Discussions

- Team Sub Representatives
  - PEO SUBS PMS 425 - (202) 781-1051
  - PEO SUBS PMS 397 - (202) 781-4430
  - NUWC Newport - (401) 832-3170