Navy Implementation of MOSAICS

MOSAICS Industry Day

Michael Kilcoyne

November 4th, 2020

Cyber Resiliency Mandates and Laws

NAVFAC is the authority responsible for/supporting with the following:

- [ASD(A&S)] **DOD Construction Agent** – 10 USC Chapter 169
- [RD&A] **Acq/Tech Authority** (SECNAVINST 5400.15C)
- [OPNAV N2N6] Manage **Cybersecurity risk** for facilities (OPNAVINST 5239.1D)
  - OPNAVINST 5239.4, "Chief of Naval Operations Cybersecurity Safety Program" describes the overall Naval CYBERSAFE program
- SECNAVINST 5239.22 establishes policy and assigns responsibilities for the development, management, and implementation of the **CYBERSAFE Program**
- DoDI 5200.44 "Protection of Mission Critical Functions to Achieve **Trusted Systems and Networks**"
- Naval Facilities Engineering and Expeditionary Warfare Center (EXWC) designated a Defense Science and Technology Reinvention Lab (**STRL**) – PL 115-91, 131 Statute 1629
- **National Defense Authorization Act (NDAA) 1649** – provide **Modeling/Simulation** support for Defensive Cyber Operations (DCO)
- **NDAA 1650** – enhance resiliency of Facility Related Control Systems (FRCS) supporting critical missions (task critical and defense critical assets and major weapons systems)
  - OPNAV N46: Primary responsible party for installation assessments, executing jointly with the Navy's Mission Assurance Assessment Program
  - NAVFAC CIO: Primary responsible party for vulnerability mitigation across our infrastructure control systems and cyber physical systems.
- **8 star Letter** (NORTHCOM, INDOPACOM) – provide **visibility** on emerging threat to FRCS
- Participation in cyber events such as **Operation Rolling Tide (ORT)** and **Task Force Cyber Awakening (TFCA)** to demonstrate the effects of cyber attacks against Operational Technology (OT)
- **CNIC/NAVFAC Joint Letter** requires hardening of control systems that support STRATCOM missions

These Requirements Form the Foundation for our Cyber Resiliency Work

Significance of Installation Cyber Resiliency

Cyber Resiliency is a *Critical Component* of Navy Defense Strategies

- National Security Strategy (DEC 2017)
- Secretary of the Navy Installation Energy Resilience Strategy (FEB 2020)
- OUSD (A&S) letter on Installation Resiliency (FEB 2020)

- **Cyber Resiliency –** the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources…Cyber resiliency is emerging as a key element in any effective strategy for mission assurance, business assurance, or operational resilience *(NIST SP 800-160 v2)*
- **Energy Resiliency –** the ability to avoid, prepare for, minimize, adapt to, and recover from anticipated and unanticipated energy disruptions in order to ensure energy availability and reliability sufficient to provide for mission assurance and readiness, including mission essential operations related to readiness, and to execute or rapidly reestablish mission essential requirements *(Section 101, Title 10, United States Code)*

Cyber Resiliency is a Prerequisite to Having Energy Resiliency

Operational View: FRCS Resilient Network Infrastructure

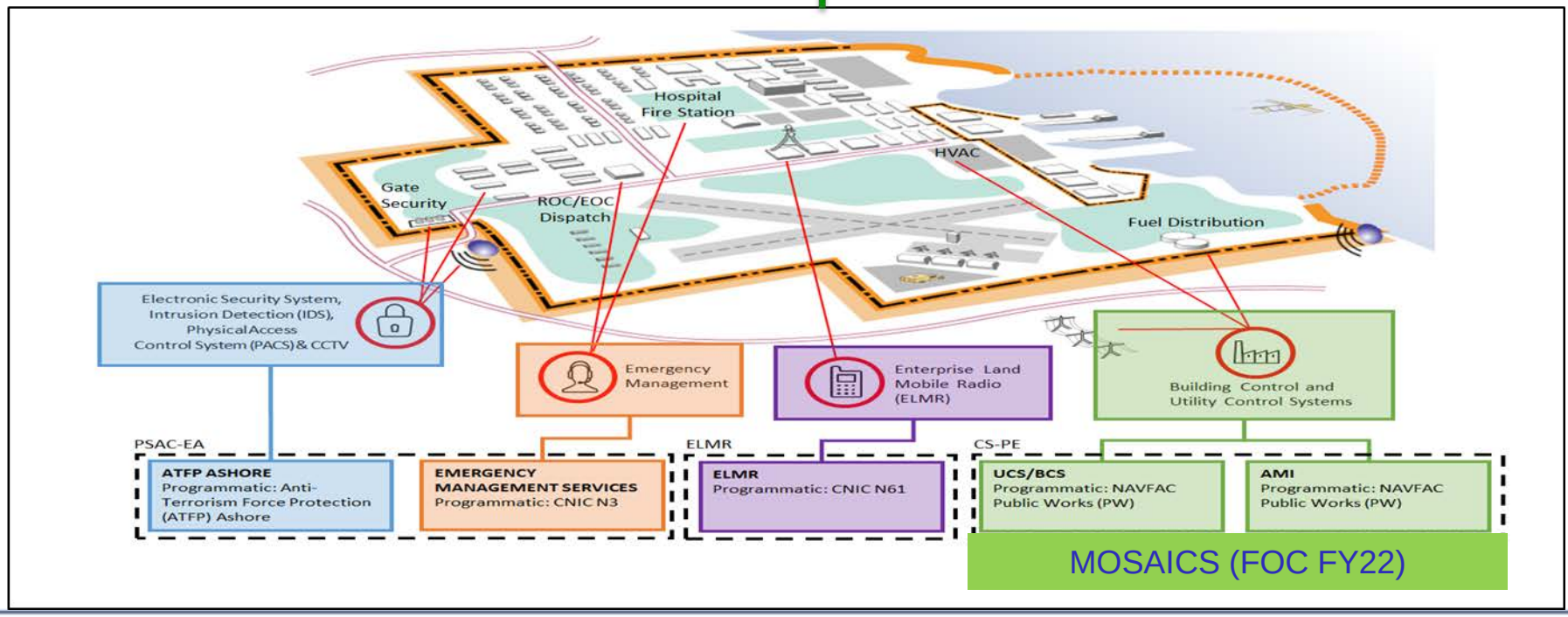
NOC
- Network Operations
- Engineering
- Helpdesk

C2SOC
- IR
- ISCM
- Protect-Defend

PSNET
- Isolated
- Failsafe
- Connect >130 installations
- Low packet loss
- Low jitter
- Low latency

Access Control List
Proxy Limited Communications
Via CNIC CESC/SDP

NIPRNet



MOSAICS-NAVFAC Implementation

MOSAICs is the capability for advanced security orchestration and automation of procedures to detect, mitigate and recover from a cyber attack on ICS networks combined with decision support, analytic, visualization, and information sharing tools

- *IOC Electrical Distribution SCADA*
  - *Current Funding for 10 Electrical Distribution Systems*
  - *Baselining tool could be used to identify FRCS components and help develop FRCS models in support of MBSE*
  - *Connect those disparate Electrical distribution systems to the Control System Platform Enclave (CSPE)*
- *FOC Entire FRCS Portfolio (Water, Power, HVAC, etc.)*
  - *300+ Systems need to be instrumented with MOSAICS and connected to the CSPE*
- *Transition MOSAICS Capability to the Anti Terrorism Force Protection (ATFP) Portfolio (ESS, Cameras, etc.)*

Capabilities Relying/Using MOSAICS

- *Model Based System Engineering for Facility Related Control Systems (FRCS)*
- *Control System Test Bed (CSTB)*
- *TTP-Based Cyber Hunt Automation for Mission Protection (T-CHAMP)*
- *Operational Technology (OT) Software Defined Networking (SDN)*
- *Cyber Protection and Reaction Cell (CPRC)*
- *Adversarial Assessment Team*
- *Incident Response Team*

Questions