Cybersecurity Program Office (PMW 130) Update to AFCEA

20 October 2020
John T. Armantrout
Program Manager (PMW 130)
858.537.0682
john.armantrout@navy.mil

DISTRIBUTION STATEMENT A: Approved for public release, distribution is unlimited (19 OCTOBER 2020)
Agenda

- PMW 130 Introduction
- What Keeps Me Up at Night
- PMW 130 AI / ML Prize Challenges
- PMW 130 S&T Cybersecurity Warfighting System (CWS) Project
- Potential Contracting Opportunities
- #GPOD
Our **vision** is to predict, protect, detect, and react to cyber threats for a secure maritime enterprise

Our **mission** is to enable Information Warfare through implementation of a fully integrated architecture providing confidentiality, integrity, and availability of capabilities through innovative acquisition of maritime cybersecurity products

Our new name and logo
The Navy’s Cybersecurity Program Office (PMW 130)

• Crypto and Key Management
  ➢ Key Management: Key Management Infrastructure (KMI), Simple Key Loader (SKL), Tactical Key Loader (TKL)
  ➢ Data and Voice Cryptography (Modernization and Legacy)
  ➢ Secure Voice: Tactical Shore Gateway (TSG)
  ➢ Public Key Infrastructure (PKI)

• Network Security
  ➢ Endpoint Security
  ➢ Computer Network Defense (CND)
  ➢ SHARKCAGE (Defensive Cyber Operations (DCO) enclave) / CND Deployer Toolkit (CDT)

• Cyber Analytics
  ➢ Vulnerability and Remediation Asset Manager (VRAM)
  ➢ Navy Cyber Situational Awareness (NCSA)
  ➢ Navy Commander’s Cyber Dashboard (NCCD)
  ➢ Readiness Analytics and Visualization Environment (RAVEN)
  ➢ Counter Insider Threat Capability (CITC)
  ➢ Navy’s Cross Domain Solution (CDS): Radiant Mercury
Agenda

• PMW 130 Introduction
• What Keeps Me Up at Night
• PMW 130 AI / ML Prize Challenges
• PMW 130 S&T Cybersecurity Warfighting System (CWS) Project
• Potential Contracting Opportunities
• #GPOD
What Keeps Me Up At Night

- Quantum Computing
- Worldwide Out-of-Band (OOB) Management Grid for U.S. Navy
  - Alignment with the Integrated Navy Operations Command and Control System (INOCCS) Framework
- Cross Domain Solutions
- Situational Awareness
  - Cyber
  - Vulnerability
- Cyber Metrics
  - Vulnerabilities per Asset (VPA)
  - Common Vulnerability Scoring System (CVSS)
  - Damage Potential (Risk)
- Comprehensive Supply Chain Risk Management Process
- Funding
- Pace of Change
- Engage
Agenda

• PMW 130 Introduction
• What Keeps Me Up at Night
• **PMW 130 AI / ML Prize Challenges**
• PMW 130 S&T Cybersecurity Warfighting System (CWS) Project
• Potential Contracting Opportunities
• #GPOD
Prize Challenges are another tool in the Acquisition toolkit to seek out innovative solutions to complex problems faced by the DoD

Anyone 18 years of age and older who is a US Citizen may submit their solution to solve the Prize Challenges

Prize amounts can be customized up to $1M USD

The Government can utilize results from the Prize Challenges to issue a sole source contract award, as the challenge results are equivalent to that of an Analysis of Alternatives (AoA)

NAVWAR has conducted two Prize Challenges to date, both executed by PMW 130 in partnership with Oak Ridge National Laboratory (ORNL)

These challenge are part of the Artificial Intelligence Applications to Autonomous Cybersecurity (AI ATAC) series of Prize Challenges
AI ATAC Overview

- The AI ATAC series of challenges seek innovative Cybersecurity solutions that leverage the power of Artificial Intelligence and Machine Learning (AI / ML) to detect unknown, sophisticated cyber attacks and assist the warfighter in combatting burnout in the Security Operations Center (SOC)

- Prize Challenge #1 - Endpoint Malware Detection
  - Focused on detecting malware on an endpoint
  - Industry-first evaluation of this scale - 100K samples (50K malicious, 50k benign) were evaluated against each tool
  - First Place: FireEye ($100K Prize)
  - Second Place: Elastic Endpoint Security ($50K Prize)

- Prize Challenge #2 - Network Detection of Adversarial Campaign Activity
  - Focuses on detection of network threats / anomalies
  - Currently being evaluated at ORNL in the Cybersecurity Operations Research Range (CORR)
  - Anticipate results in mid-November 2020
  - First Place Prize is $500K (winner takes all)

- Prize Challenge #3 - SOC Automation
  - Focuses on automating the SOC using Security Orchestration, Automation, and Response (SOAR) tools
  - Evaluation framework is currently in development
  - Anticipate announcement in Q1FY21
  - First Place Prize is $750K (winner takes all)
Agenda

• PMW 130 Introduction
• What Keeps Me Up at Night
• PMW 130 AI / ML Prize Challenges

• PMW 130 S&T Cybersecurity Warfighting System (CWS) Project

• Potential Contracting Opportunities
• #GPOD
The CWS project aims to inform the INOCCS Framework design by evaluating Denied, Disconnected, Intermittent, and Limited Bandwidth (D-DIL) environmental impacts on cloud-based commercial off-the-shelf (COTS) cybersecurity products

- The CWS project will conduct a series of experiments to evaluate alternative architectures, dataflows, and workflows for cyber defense of intermittently-connected afloat platforms
- CWS intends to perform these evaluations in cooperation with FCC/C10F personnel, conducting Live / Virtual / Constructive (LVC) events within the Persistent Cyber Training Environment (PCTE) and / or the National Cyber Range Complex (NCRC)

As a derived result, this project seeks to demonstrate viability of cooperative cyber range events where FCC/C10F personnel can directly interact with PMW 130's design concepts under development

- CWS may create new business opportunities for SOAR, Endpoint Detection and Response (EDR), Security Information and Event Management (SIEM), and data broker vendors
• PMW 130 Introduction
• What Keeps Me Up at Night
• PMW 130 AI / ML Prize Challenges
• PMW 130 S&T Cybersecurity Warfighting System (CWS) Project
• Potential Contracting Opportunities
• #GPOD
Potential Contracting Opportunities

• SHARKCAGE
  - Globally distributed, passive, isolated, and cryptographically separated collection of classified information systems that support the U.S. Navy’s Defensive Cyberspace Operations – Internal Defensive Measures (DCO-IDM) missions
  - Completed review of 17 RFI responses
  - RFP tentatively planned for Q2FY21
    - Establish a single integrated modular solution scalable for both ashore and afloat operational support platforms
    - Address an enterprise solution across all mission enclaves
    - Alignment with INOCCS Framework

• VRAM
  - COTS solution to provide a web-enabled network vulnerability data repository, asset management, monitoring, and analysis tool and serve as the Navy’s authoritative Cyber Directive compliance reporting tool
  - Completed review of 14 RFI responses; in process of completing a COTS alternatives market research report

• PMW 130 Cybersecurity Engineering, Technical and Program Management Support Services
  - Planned contract award 2QFY22
Agenda

• PMW 130 Introduction
• What Keeps Me Up at Night
• PMW 130 AI / ML Prize Challenges
• PMW 130 S&T Cybersecurity Warfighting System (CWS) Project
• Potential Contracting Opportunities
• #GPOD
The GPOD Pledge

• My Job #1 is to “support” the Fleet. [This has many different meanings depending on your roles and responsibilities – but it all ties back to Job #1].

• I will work to eliminate “speed bumps” keeping me from delivering product and will report up my chain of command anything hindering me from delivering my product.

#GPOD

• I will do my absolute best to deliver product – on time and on budget.

• If I need additional resources to deliver product on time and on budget, I will ask for them.

• I will think of [legal] new and different ways to ensure on time and on budget delivery of product – I will be innovative!

• When I make a commitment, I keep that commitment.
Accelerated delivery of required capability that is affordable, integrated, and interoperable