Product Manager
Cyber Platforms and Systems (CPS)
Collaboration with Industry Event

LTC Bradley Son, Product Manager (PdM)
Mr. Anthony Howard, Deputy Product Manager(DPdM)

28 March 2023

Agenda

- LTC Son Introduction
- Purpose
- High Level Stakeholders
- DCO Operational Overview
- Top Goals and Priorities
- Deployable Defensive Cyberspace Operations System – Modular (DDS-M)
- Garrison Defensive Cyberspace Operations Platform (GDP)
- Forensics and Malware Analysis (F&MA)
- Counter Infiltration (CI)
- Technical Management Division (TMD)
- Defensive Cyberspace Operations Tools Suite (DCO Tools Suite)

Cyber Platforms and Systems (CPS)

Cyber Platform & Systems (CPS) focuses on the procurement and delivery of cyber platforms and cybersecurity tools for the Armed Forces. The cyber platform is the foundational piece of equipment used by Cyber Soldiers. It allows them to conduct maneuvers on cyber terrain and affect Department of Defense Information Network (DODIN) defense.

MISSION

Support Cyber Defenders – Rapidly Acquire and Deliver Innovative, Proven and Tested Capability – Protect the Infrastructure, Preserve Security, and Achieve Information Advantage – Support Defense Cyber Operations.

Product Manager CPS
LTC Bradley Son

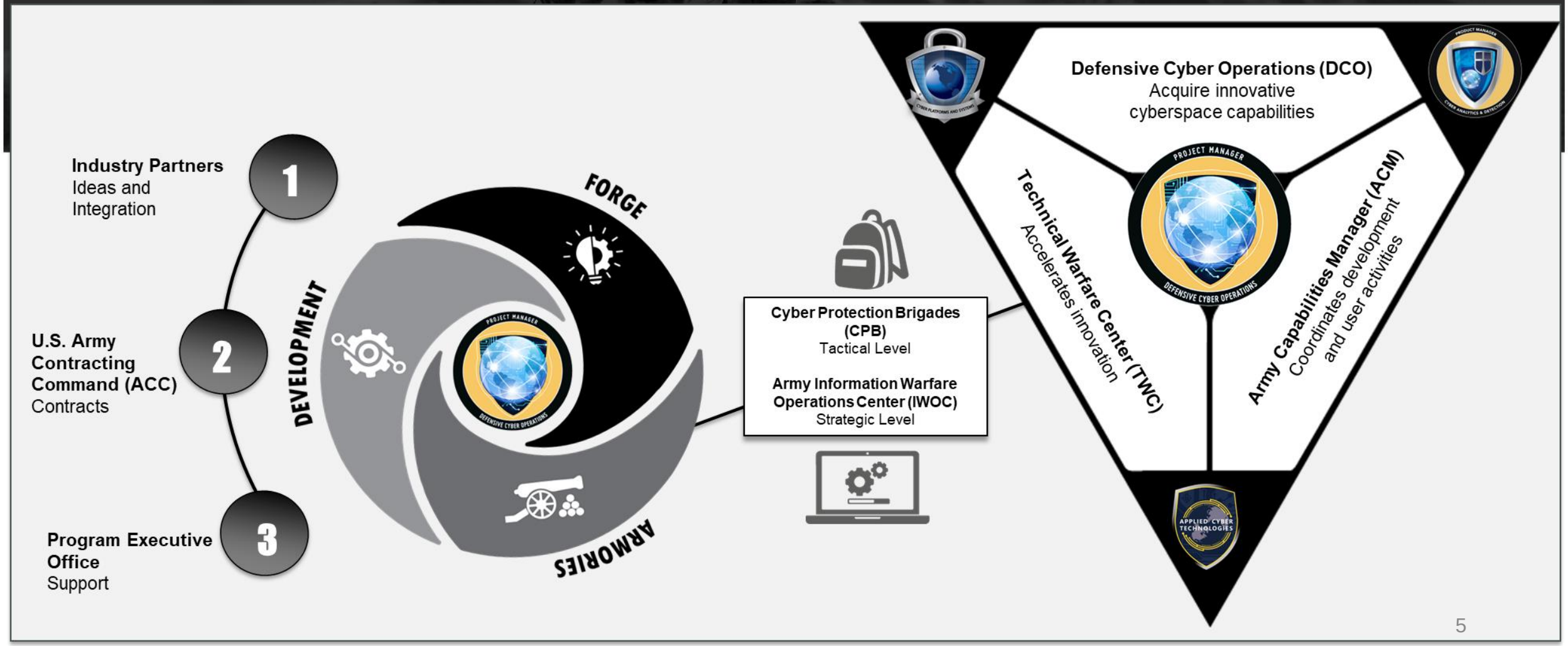
What is the Purpose

Collaboration with Industry

Provide Industry partners with an overview of Cyber Platform and Systems (CPS) Programs of Record. Industry partners will have the opportunity to ask questions, share feedback about and engage directly with Cyber Platform and Systems Leadership and Assistant Product Managers

Defensive Cyber Operations (DCO)
High Level Stakeholders

WORKING TOGETHER TO DEFEND THE ARMY'S NETWORKS FROM CYBERSPACE ATTACKS



Defensive Cyber Operations (DCO)
Operational Overview

Cyber Analytics (CA)

Big Data Platform (Gabriel Nimbus)

presence of complex threats and vulnerabilities
- Ingest large amounts of data

DCO Mission Planning (DCOMP)
- Supports mission planning and situational awareness for Cyber Wargaming, Analyses, Training, Network Visualization
- Coordinating with Joint solution for increased efficiencies and shared capabilities

User Activity Monitoring (UAM)
- Identifies and malicious activity
- Monitors Insider Threats

Counter Infiltration (CI)
- Deceive the Enemy (Reconnaissance) and Detect Intrusions. Allows an operator to monitor the adversary's behavior

Threat Emulation (TE)
- Model enemy activity for training and wargaming
- Environments are in a garrison, deployed, or mission partner setting.

Defensive Cyberspace Operations Tools Suite
- Software used to detect intrusion and conduct analysis
- Tools are used and developed in all 3 platforms below
- Over 100 tools several are acquired for advanced threats
- Tools continually change as new requirements emerge
- 100% of the tools are available 100% of the time

Forensics and Malware Analysis (F&MA)
- Rapidly triages cyber-incidents and performs analysis and collection of malicious data. (malware)
- After the fact assessment and resolution
- a trace to source solution and a containment solution.

PLATFORMS

Deployable DCO System (DDS)

(DEPLOYABLE)
Configurable hardware kit, can be easily fit in an aircraft overhead compartment. It is armed with the ability to tap into a network and host tools for defensive measures.

Garrison DCO Platform (GDP)

(FIXED)
Provides remote operational capabilities and a common platform. It has the ability to integrate with the Big Data Platform, Global Enterprise Fabric and cloud environments.

Emerging Capabilities

Security Automation Orchestration and Response (SOAR): Automated Internal Defense Measures for Evolving Threats

The employment of defensive capabilities achieve the following objectives: deter, destroy and defeat cyberspace threats; gain time; economy of force; control key terrain; protect tasked critical assets and infrastructure; and develop intelligence

Deployable Defensive Cyberspace Operations System – Modular (DDS-M)

Cyber Platforms and Systems (CPS)

Supporting Defensive Cyber Operations

Where we are today

- We are currently prototyping the next generation DDS-M using the lessons learned from the previous version to improve the capability for the Cyber Defender

Where we need to be

- We need to deliver a capability that focuses on ease of use and modularity in a way that makes it easily adaptable to meet evolving mission requirements (scalable)

Where industry can help

- Industry can help by providing the Government with cutting edge solutions to solve complex technological problems through the integration of Commercial off the Shelf solutions.

Supporting Big Army

- Collaborate with the Air Force, Marines, Navy and USCC to help shape how Cyber Command converges to manage all Active Cyber Forces scheduled for FY24

- Lead the effort to shape what a joint solution will look like for FY24 by leveraging the USCC Hunt Forward OTA to rapidly assess and field the next generation DDS M capability

Garrison Defensive Cyberspace Operations Platform (GDP)

Cyber Platforms and Systems (CPS)

Supporting Defensive Cyber Operations

Where we are today

- Currently have multiple GDPv3 systems in the field
- Completed testing of the next iteration of the GDP platform, the GDPv4

Where we need to be

- GDPv4 systems installed at ARCYBER identified locations and added to additional ATOs
- Additional tools added to the GDPv3 system

Where industry can help

- Provide better methods for ongoing RMF for the systems
- Provide a method for better TAP strategies for data ingest

Supporting Big Army

GDPv3

- Systems are installed in multiple theaters of operations.
- Ingesting data from the network to allow cyber defenders to remotely connect to them to complete their mission

GDPv4

- Planning for installs in multiple theaters of operation
- Will be the hardware basis for SIEM
- Will provide the ability to connect with / send data to Gabriel Nimbus

Forensics and Malware Analysis (F&MA)

Cyber Platforms and Systems (CPS)

Supporting Defensive Cyber Operations

Where we are today

- The current F&MA solution is being assessed to ensure that it fully meets the various requirements for our Cyber Defenders.

Where we need to be

- Begin deploying an F&MA capability across ARCYBER and RCCs by 2QTR FY23.

Where industry can help

- Demo enterprise solutions (1 tool) that perform both forensics and malware analysis automatically.

Supporting Big Army

Forensics and Malware Analysis:

Provides the ability to perform forensics analysis locally and remotely in order to detect, identify, and respond to attacks. The capability pushes forensics analysis forward to the Regional Cyber Centers (RCC) in order to perform live box forensics. Live box forensics allows the capture of volatile memory critically needed during an incident response.

Counter Infiltration (CI)

Cyber Platforms and Systems (CPS)

Supporting Defensive Cyber Operations

Where we are today

- Requirement Definition Package approved in January 2023
- Building deployment plan and strategy

Where we need to be

- In procurement of CI capability
- Starting RMF activities or reciprocity from DODIN-A APL

Where industry can help

- Explore potential enterprise solutions for CI

Supporting Big Army

Counter Infiltration:

The CI capability provides decoy systems, files, credentials and other baits/lures in order to provide early warning and detection. Cyber defenders will use the capability to detect, identify, and respond to adversary interactions with deception countermeasures in defense of the Department of Defense Information Network (DODIN) and the Army (DODIN-A) network.

Technical Management Directorate (TMD)
Forge & Armory
Cyber Platforms and Systems (CPS)

Supporting Defensive Cyber Operations

Where we are today

- Recently collapsed ACT into CPS and formed the Technical Management Directorate (TMD) under CPS – same great people, same great service!
- TMD Forge & Armory Concept
  - **Forge (FGGA):** Provides expertise in areas of engineering, RMF, and SCRUM to each APM through cross functional teams
  - **Armory (FBVA/FGGA/PA):** 3x eastern U.S. sites led by TYAD teams who provide helpdesk, logistical, and maintenance support for DCO portfolio

Where we need to be

- Forge R&D emerging technologies to enhance the Army's DCO capabilities
- Armory provides asset visibility and usage analytics of both hardware and software through implementation of ServiceNow

Where industry can help

- Provide opportunities for collaboration and development of leading-edge commercial solutions

Supporting Big Army

Forge

- ***Interfaces and collaborates*** with ARCYBER, CYBERCOM, and outside agencies to mature and develop commercial capabilities
- ***Synchronizes*** both hardware and software development, and manages implementation plans
- ***Provides oversight*** of Armory to rapidly address system performance issues

Armory

- ***Interfaces and integrates*** with COMPO I, II, and III units
- ***Provides end-user support*** through Tier III helpdesk support and depot level maintenance
- ***Manages asset visibility*** for DCO portfolio, and provides performance analytics for hardware and software systems

Defensive Cyberspace Operations Tools Suite (DCO Tools Suite)

Cyber Platforms and Systems (CPS)

Supporting Defensive Cyber Operations

Where we are today

- Supplying DCO Tools to CPS along with supporting SW capabilities and training to Cyber Protection Teams

Where we need to be

- Single pane of glass: Synchronized DCO capability with truly unified tools across the enterprise

Where industry can help

- Focus on synchronization solutions vs. individual tools
- Help expedite the RMF process by proactively getting ahead of artifact collection and securing approval to connect

Supporting Big Army

Security Information Exchange Management (SIEM)

- Unified SIEM (U-SIEM) deployment to all Regional Cyber Centers in support of future Unified Network Operations (UNO)

Security Orchestration Automated Response (SOAR)

- Deploying SOAR capability to Gabriel Nimbus

Supervisory Control & Data Acquisition (SCADA)

- Evaluation activities underway to identify and provide a SCADA solution to the Army 3/4Q FY23

Q & A

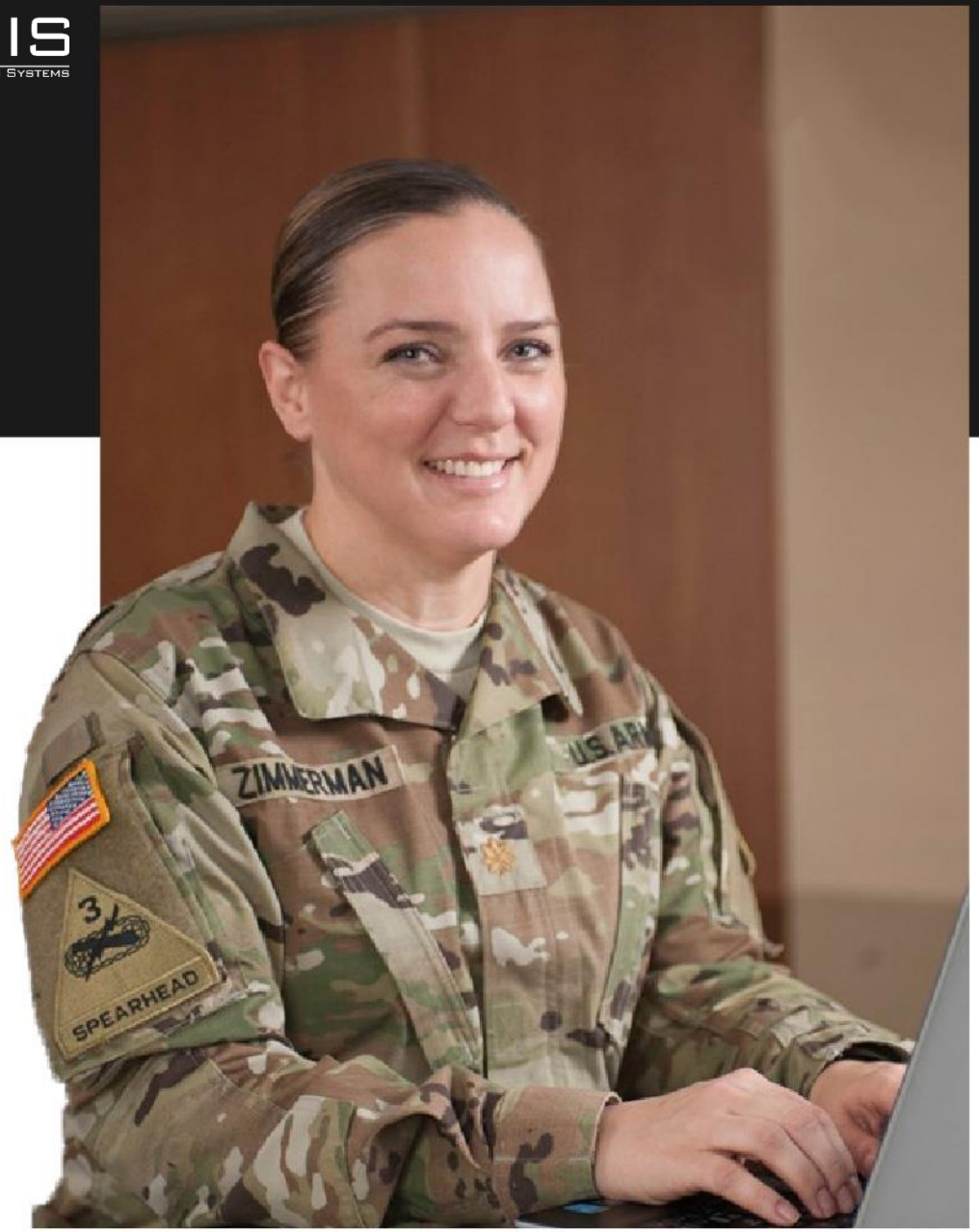
What are your Questions?

For procurement opportunities:

https://www.eis.army.mil/opportunities

These Slides

https://www.eis.army.mil/newsroom/publications



CYBER PLATFORMS AND SYSTEMS

MEET WITH US

theforge.force.com/peoeis/s/

CONNECT WITH US

eis.army.mil/mission-areas/cps

Company/ArmyDCO

DCO-CPS@army.mil