Product Manager
Cyber Platforms and Systems (CPS)
Discussion and Overview with
U.S. Army Cyber Command

LTC Bradley Son, Product Manager
MAJ Matthew Sherburne, TWC DCO Division Chief

November 9, 2022

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.

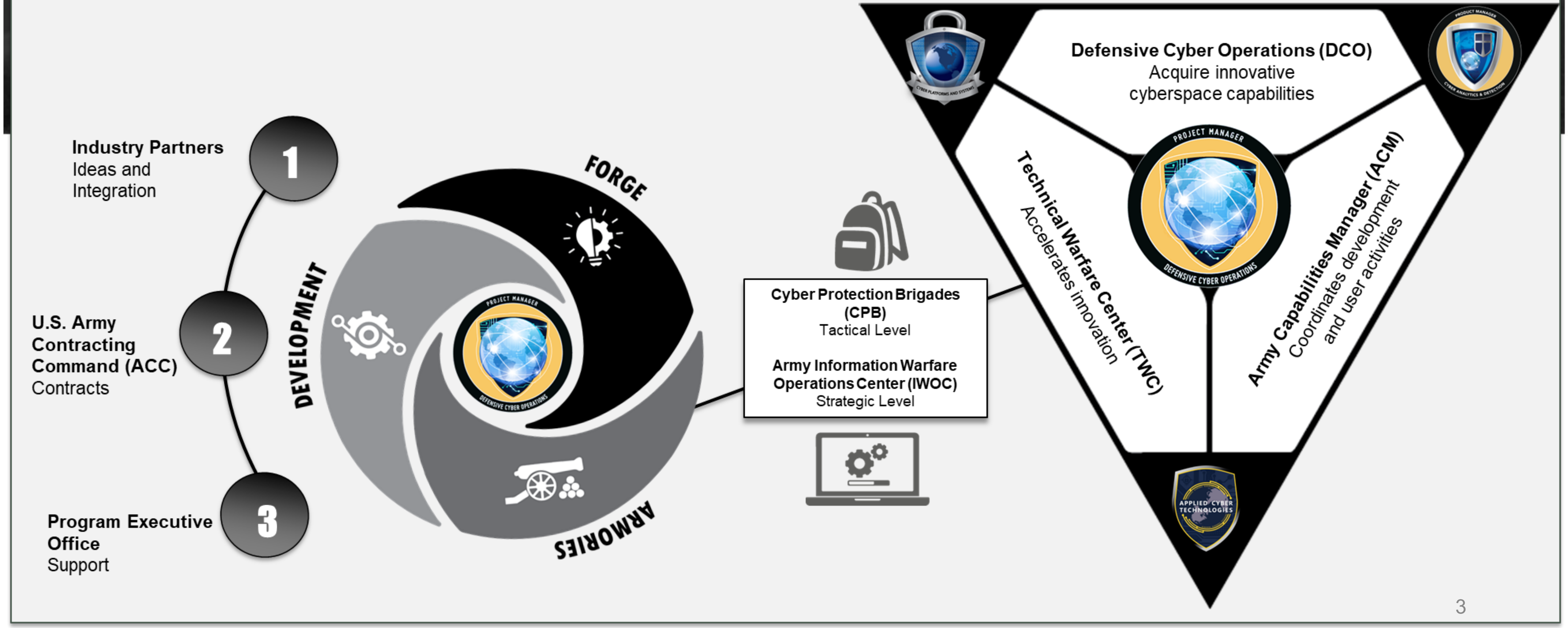
MISSION

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

Defensive Cyber Operations (DCO) High Level Stakeholders

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



1 **Industry Partners**
Ideas and Integration

2 **U.S. Army Contracting Command (ACC)**
Contracts

3 **Program Executive Office**
Support

Cyber Protection Brigades (CPB)
Tactical Level

Army Information Warfare Operations Center (IWOC)
Strategic Level

Defensive Cyber Operations (DCO)
Acquire innovative cyberspace capabilities

Technical Warfare Center (TWC)
Accelerates innovation

Army Capabilities Manager (ACM)
Coordinates development and user activities

CYBER PLATFORMS AND SYSTEMS
PRODUCT MANAGER
CYBER ANALYTICS & DETECTION
APPLIED CYBER TECHNOLOGIES

U.S. Army Cyber Command

Technical Warfare Center (TWC) Defensive Cyber Operations (DCO) Division

Mission: Technical Warfare Center (TWC) Defensive Cyber Operations (DCO) Division orchestrates, facilitates and ensures integrated capability development and delivery to U.S. Army Cyber Command (ARCYBER) forces.

Vision: Continuous integration of operational and institutional activities enabling Army DCO Forces to be equipped for decisive operations and empowered to rapidly innovate.

U.S. Army Cyber Command
Technical Warfare Center (TWC) Capability Development

- **Material solution focused**. Initial Capability Document (ICD) – a requirements document that satisfies a defensive cyber need based on gap analysis.

- Serve as the **direct program conduit** with Army Capability Manager (ACM) Cyber and designated materiel developers.

- Serve as the **capability integrating activity** for the Army DCO Community of Interest (COI):
  - Help each COI understand what programs are being delivered, on what schedule, and if it meets the requirement.
  - Work with stakeholders to deliver what is needed as close as possible to when it is needed.

- Serve as the lead coordinator to **facilitate capability alignment from inception to delivery** within ARCYBER Commanding General (CG) and Chief Technical Officer (CTO) guidance and priorities.

- Responsible for **requirements validation** and **assisting solutions analysis** for Capability Needs Requests (CNRs) through support and operations channels.

- Assist ARCYBER staff by recommending capability development and support priorities based on metrics and assessed operational value.

Defensive Cyber Operations (DCO)
Operational Overview

US ARMY PEO EIS
PEO ENTERPRISE INFORMATION SYSTEMS

Cyber Analytics (CA)

Big Data Platform (Gabriel Nimbus)

- Facilitates counter-reconnaissance activities, discover the 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

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.

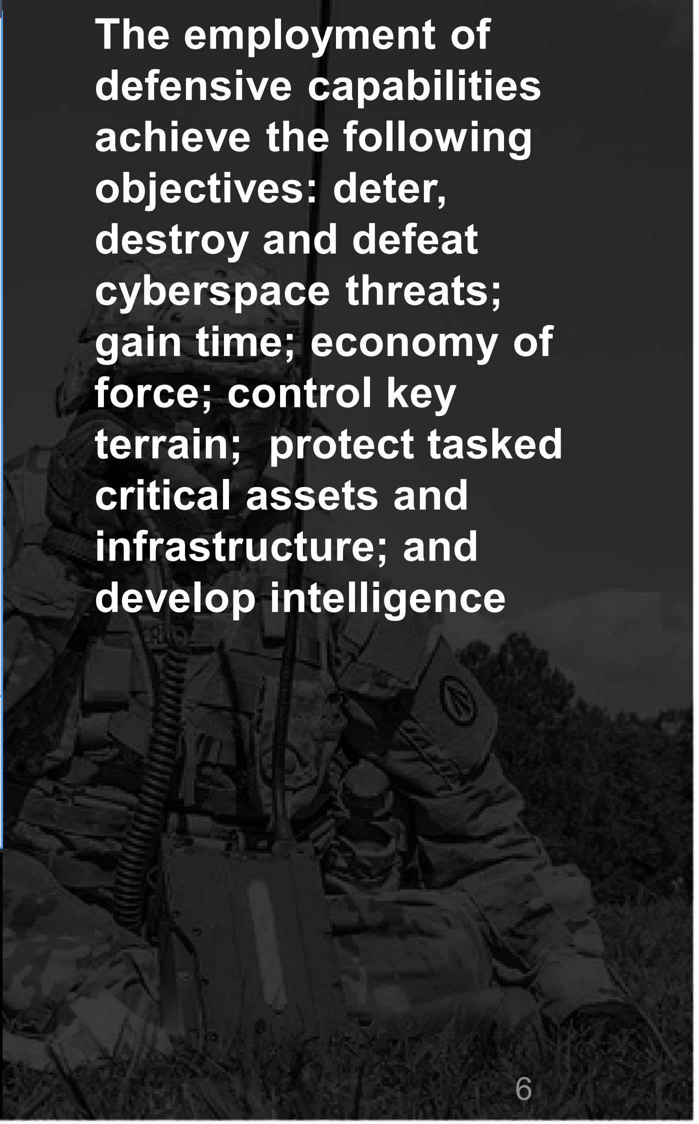
Garrison DCO Platform (GDP)

(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

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

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

Cyber Platforms and Systems

Innovative | Integrated | Effective

TOP GOALS & PRIORITIES

- Provide operational capability to the Army Cyber Command's Cyber Protection Brigades allowing for rapid evaluation and response to unexpected and dynamic cyber threats.

- Provide the ability to rapidly triage an incident and place the impacted system back in service. A portable capability enables cyberspace defenders to quickly review information stored on deployed computers in real-time – without altering or damaging it.

- Deliver new prototype solutions allowing deployment in austere environments to defend the Department of Defense Information Network (DoDIN)

US ARMY PEO EIS
PEO ENTERPRISE INFORMATION SYSTEMS

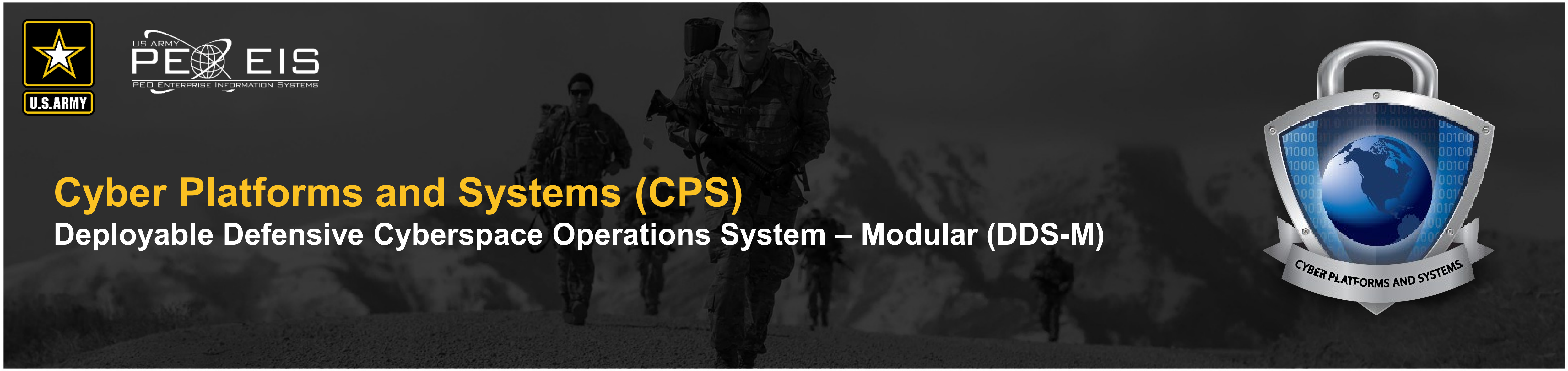
CAPABILITIES

Deployable Defensive Cyberspace Operations Systems-Modular (DDS-M)
Is a configurable hardware kit that can be easily fit in an overhead compartment of an aircraft.

Garrison Defensive Cyberspace Operations Platform (GDP)
Provides remote operational capabilities and a common platform between DCO and Department of Defense Information Network-Army (DoDIN-Army) systems.

Defensive Cyberspace Operations Tools Suite (DCO Tools Suite)
Integrates Commercial Off-the-Shelf (COTS) and open-source software (OSS) tools and products and continually leverages the user assessment approach

Forensics and Malware Analysis (FM&A)
Forensics provides the ability to rapidly triage cyber-incidents and perform forensics analysis and collection remotely or locally.



US ARMY PEO EIS
PEO ENTERPRISE INFORMATION SYSTEMS
U.S. ARMY
CYBER PLATFORMS AND SYSTEMS

Cyber Platforms and Systems (CPS)

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

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 but can be easily adapt to meet evolving mission requirements

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

Cyber Platforms and Systems (CPS)

Garrison Defensive Cyberspace Operations Platform (GDP)

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

Cyber Platforms and Systems (CPS)

Defensive Cyberspace Operations Tools Suite (DCO Tools Suite)

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 NETOPS capability with truly unified tools across the enterprise

Where industry can help

- Focus on synchronization solutions vs. 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)

- NextGen SIEM deployment to Regional Cyber Centers Pacific & Europe in support of future Unified Network Operations (UNO)

Security Orchestration Automated Response (SOAR)

- Deploying SOAR to Gabriel Nimbus

Supervisory Control & Data Acquisition (SCADA)

- Prototype activities underway to identify and provide a SCADA solution to the Army this Spring

Cyber Platforms and Systems (CPS)

Forensics and Malware Analysis (F&MA)

Supporting Defensive Cyber Operations

Where we are today

- EnCase Endpoint Investigator Deployment (EEI) Planning beginning with RCC-C Ft. Carson and Ft. Bragg Nov ’22
- Provide training EEI training to 24 trainees in RCCs, CPB and ARCYBER F&MA Cell

Where we need to be

- EEI is fully deployed across ARCYBER and RCCs by 4QTR FY24

Where industry can help

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

Supporting Big Army

Providing live box forensics across the enterprise

- TBD

Cyber Platforms and Systems (CPS)

Counter Infiltration (CI)

Supporting Defensive Cyber Operations

Where we are today

- Requirements stage - RDP submitted for worldwide staffing
- Waiting on requirements from ACM
- Building deployment plan and strategy

Where we need to be

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

Where industry can help

- Explore potential enterprise solutions for CI

Supporting Big Army

Counter Infiltration pending signed RDP

- TBD

For procurement opportunities:

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

These Slides

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

MEET WITH US

🌐 theforge.force.com/peoeis/s/

CONNECT WITH US

🌐 eis.army.mil/mission-areas/cps

in Company/ArmyDCO

✉ DCO-CPS@army.mil