DEFENSIVE CYBER OPERATIONS (DCO)

AFCEA BELVOIR LUNCHEON

22 June 2022

Presented by:
COL Mark Taylor, PM DCO

Defensive Cyber Operations

Defensive Cyber Operations (DCO) rapidly delivers innovative and dominate cyberspace capabilities, as well as tailored information technology solutions for our national, joint and allied partners. We are the leader within the cyberspace domain; delivering innovative, integrated and cost effective solutions.

COL Mark Taylor
Project Manager DCO

LTC Dakota Steedsman
Product Manager
CAD

LTC Bradley Son
Product Manager
CPS

Mr. Arthur Edgeson
Product Lead
ACT

Mr. John Swart
Product Lead
TAO

Mr. Brian Bricker
Acting Product Lead
AIT

Defensive Cyber Operations (DCO)
Who We Are

WHAT DOES DEFENSIVE CYBER OPERATIONS DO?

- Provide cyber analytics and detection for cyber threats
- Provide deployable and cloud based defensive cyber solutions
- Provide rapid prototyping capabilities for rapid acquisition
- Foreign military sales - building partner relationships
- Command, Control, Communications, Computers and Intelligence (C5I) acquisition services

TOP GOALS & PRIORITIES

To deter or defeat enemy offensive cyberspace operations.

Acquire critical capabilities allowing the Army to maneuver with agility to decisively engage the adversary in the cyberspace domain.

To support our Active Duty, Reserve Component and National Guard cyber warriors

To proactively engage with industry and our stakeholders to create positive communication engagement at all levels.

US ARMY PEO EIS
PEO Enterprise Information Systems

MISSION

Rapidly deliver innovative and dominant cyberspace capability and tailored information technology solutions to national, joint, and allied partners to provide decisive, warfighting information advantage.

WHO WE ARE

Cyber Analytics and Detection (CAD)
Analyze | Identify | Mitigate

Cyber Platforms and Systems (CPS)
Powerful | Adaptive| Responsive

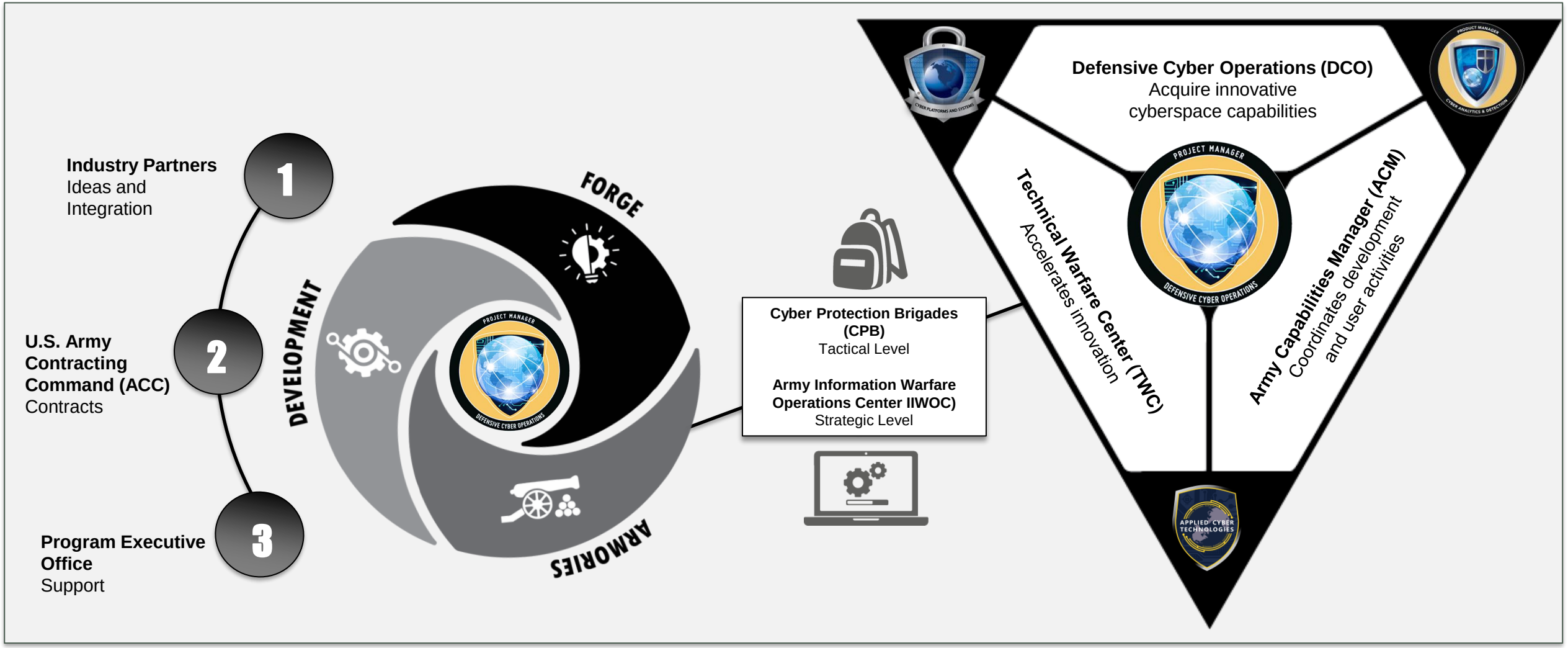
Applied Cyber Technologies (ACT)
Advance | Incorporate | Maintain

Allied Information Technologies (AIT)
Assist | Build | Train

Technology Application Office (TAO)
Communicate | Control | Defend

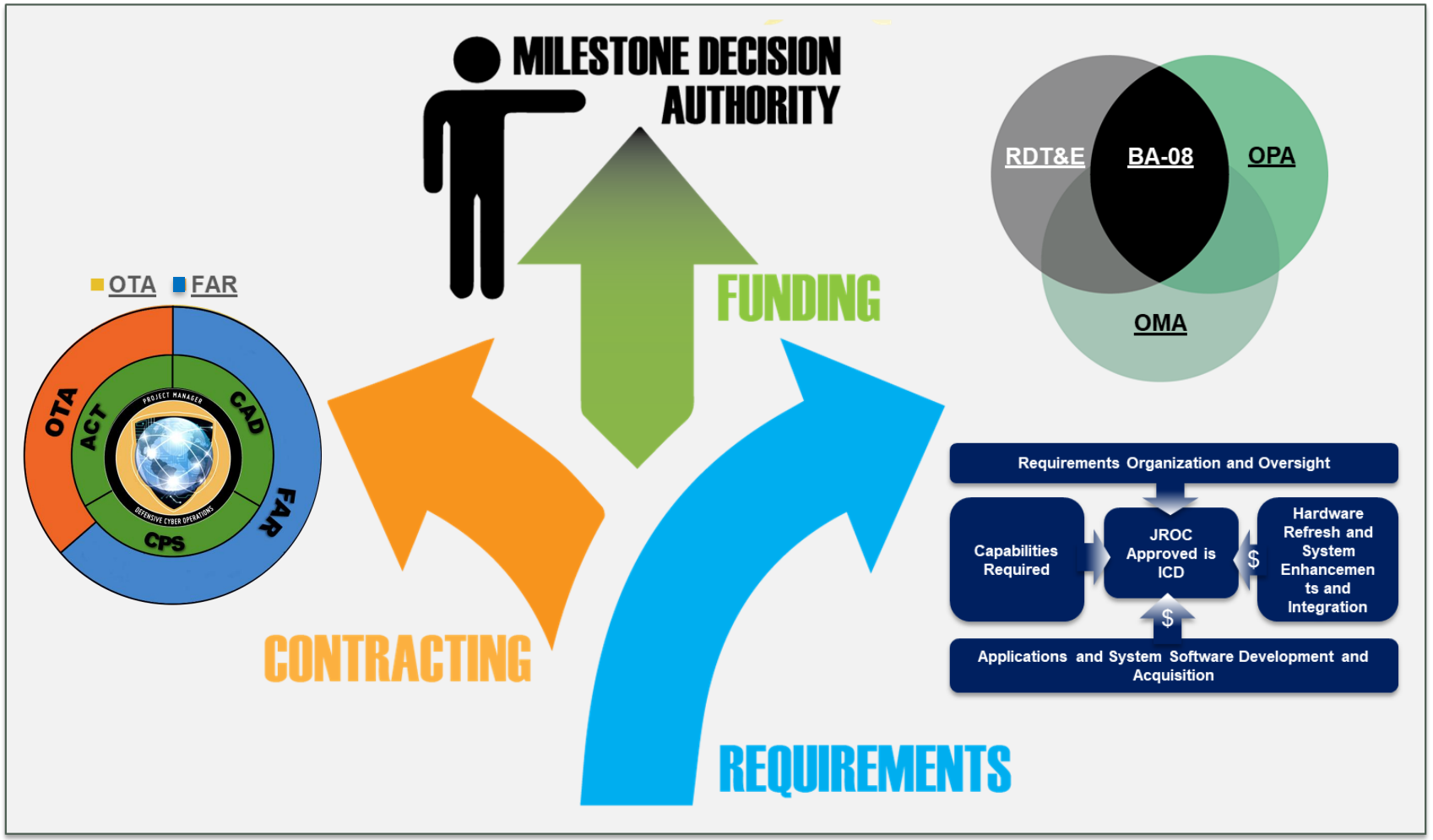
Defensive Cyber Operations (DCO)
High Level Stakeholders

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



Defensive Cyber Operations (DCO)
System Engineering Modernization

FUNCTIONAL AREA	RECOMMENDATION
Requirements	Ensure requirements allow for flexibility
Contracts	Dynamic enough to align with technological changes
Funding	Be sure funding is flexible enough to align with technological changes (BA-08 Pilot)
Funding and Milestone Decision Authority	**PROJECT MANAGER**



Defensive Cyber Operations (DCO) Requirements & Acquisition Authorities

Organization & Oversight
Army Requirements Oversight Council (AROC) Review Board (ARB)
HQDA G-8 Force Development
2-Star Board

Capabilities and Initial Minimum Values
- *Maneuver*
- *Detect*
- *Assess*
- *Etc.*

IT Box Framework (5 years)

Hardware Refresh and System Enhancements & Integration
Per Year Cost: $XXM
5 Year Lifecycle Cost: $XXM

Application and System Software Development
Per Year Cost: $XXM
5 Year Lifecycle Cost: $XXM

Acquisition Authorities

- Each RDP equates to an Acquisition Category IV (ACAT IV) Program of Record (PoR)
- PM DCO maintains Milestone Decision Authority (MDA) for PM DCO's portfolio of eight (8) ACAT IV PoRs

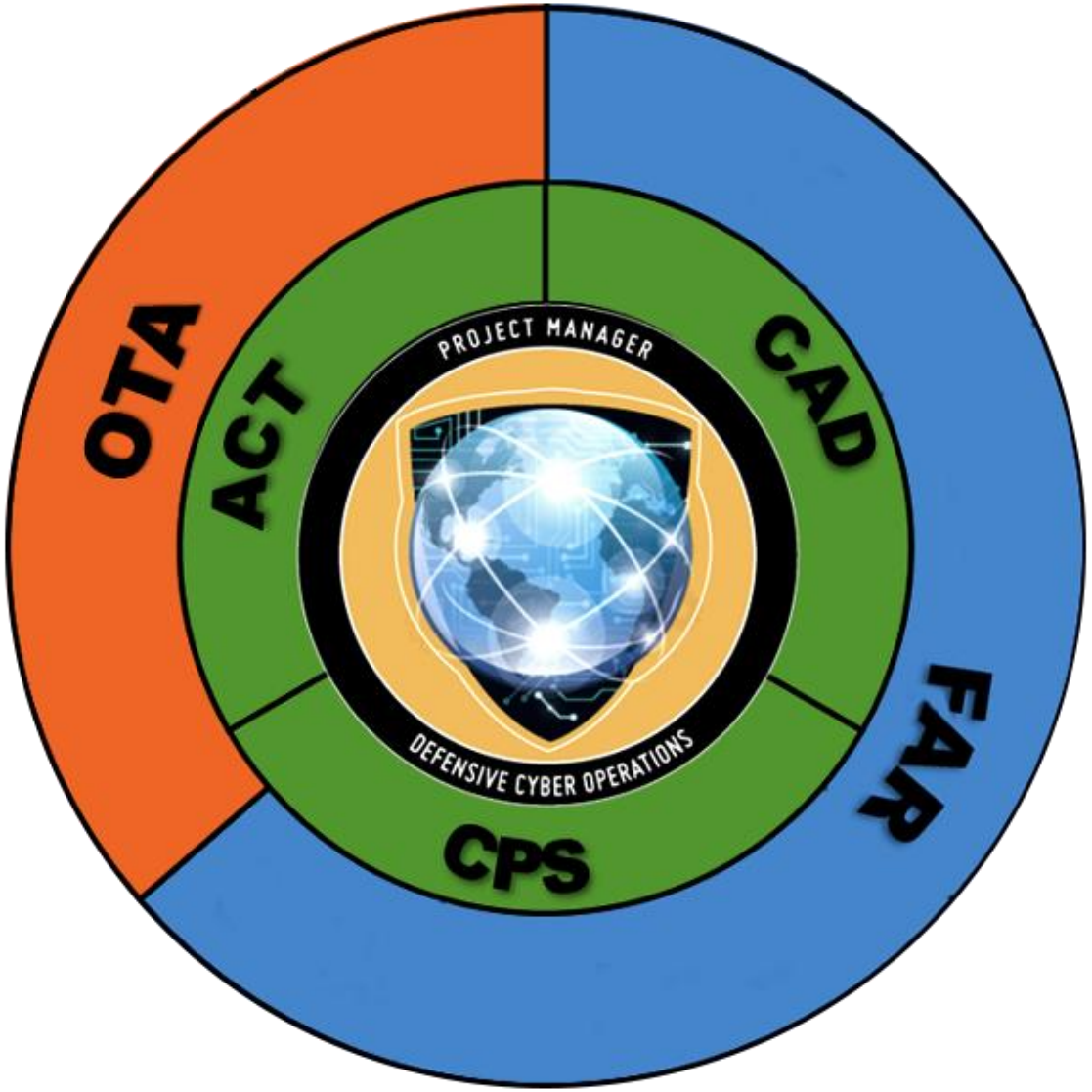
Requirements Approval Authorities

- Joint Requirements Oversight Council (JROC) Approved the DCO Info Systems Initial Capabilities Document DCO IS ICD (FY18-22) w/ IT Box Framework
- HQDA G-8 FD Approved Requirements Definition Packages (RDP)
- US Army Cyber Center of Excellence or ARCYBER Commander Approves Capability Drops (CD)

Approved DCO Approved RDPs

- Garrison DCO Platform (GDP)
- Deployable DCO System (DDS)
- DCO Tools Suite
- Cyber Analytics
- DCO Mission Planning
- Forensics and Malware Analysis
- User Activity Monitoring (UAM)
- Threat Emulation (TE)
- Tactical Defense Infrastructure

Defensive Cyber Operations (DCO) Acquisition Strategies



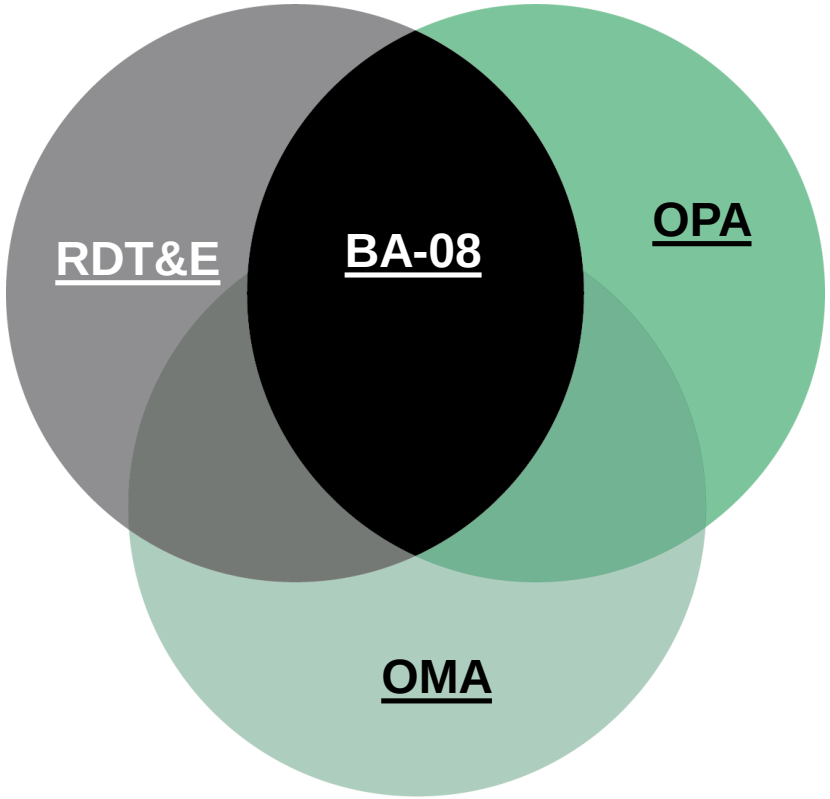
Other Transaction Authorities (OTA)

- Prototypes
- Emerging Technologies
- Technologies that need an Authority to Operate

Federal Acquisition Regulation (FAR)

- Support
- Systems Engineering and Technical Assistance (SETA)
- Integration
- Sustainment

Software and Digital Technology Budget Activity 8 (BA-08) Flexibility with Funding and the BA-08 Pilot



Areas we plan to explore as we move forward:

Acquisition is spread across three separate appropriations categories: Research, Development, Test and Evaluation (RDT&E); Other Procurement Army (OPA); and Operations and Maintenance Army (OMA).

The pilot effort realigns funding within RDT&E for selected and funded Programs of Record (PoRs).

The BA-08 effort enables the use of one appropriation type to execute software and technology activities commonly funded with three different appropriations:

The new funding mechanism aims to remove just one of many challenges program managers face when attempting to apply modern software development techniques and improve outcomes.

Defensive Cyber Operations (DCO)
Operational Overview

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 Threat for SIPRNet, JWICS, SAP

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.

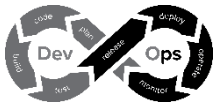
PLATFORMS AND DEVELOPMENT

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.



DCO Development Environment (DCODE)

(Innovation and Deployment)
Forge (Develop), Armories (Deploy), Development Environment (Training, Testing and Integration)

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

Defensive Cyber Operations (DCO)
Projected FY22/23 Contracting Actions
Future Requirements

FY22/23 Contracting Actions	Type	Estimated Award Date
DDS-M Additional Nodes	Production	Jul 2022
Tools SCADA Solution	Prototype	Jul 2022
SOAR OTA	Production	Jul - Aug 2022
New Euipment Training (NET)	Production	Aug 2022
Garrison Defense Platform Version 4 (GDPv4)	Production	Aug 2022
Counter Infiltration	Production	Aug 2022
Next Generation DDS-M	USCC OTA	Aug 2022
Labyrinth v3	Prototype	Aug 2022
Castle Keep (Small Set-a-Side)	FAR	Aug 2022
Laptop Refresh (CHESS)	FAR	Aug 2022
Forge Internet and Video Upgrade (TBD)	FAR	Aug –Sep 2022
GN Expansion III (1-year)	FAR	Oct 2022
Future Garrison Defense Platform (GDP) Effort	OTA	2/3 QTR FY23

Please view our upcoming procurement forecast and opportunities here:
https://www.eis.army.mil/opportunities
https://vulcan-sof.com