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.

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

Collaboration and innovation are at the core of our mission. DCO is dedicated to delivering leading-edge technology and solutions to support the cyber needs of our nation's defense.
Rapidly deliver innovative and dominant cyberspace capability and tailored information technology solutions to national, joint, and allied partners to provide decisive, warfighting information advantage.

MISSION

WHO WE ARE

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

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

Applied Cyber Technologies (ACT)
Advance | Incorporate | Maintain

Allied Information Technologies (AIT)
Assist | Build | Train

Technology Application Office (TAO)
Communicate | Control | Defend

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.
Defensive Cyber Operations (DCO)  
High Level Stakeholders

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

Industry Partners  
Ideas and Integration

U.S. Army Contracting Command (ACC)  
Contracts

Program Executive Office  
Support

Defensive Cyber Operations (DCO)  
Acquire innovative cyberspace capabilities

Technical Warfare Center (TWC)  
Accelerates Innovation

Army Capabilities Manager (ACM)  
Coordinates Development and User activities

Cyber Protection Brigades (CPB)  
Tactical Level

Army Information Warfare Operations Center (IWOC)  
Strategic Level
## Defensive Cyber Operations (DCO) System Engineering Modernization

<table>
<thead>
<tr>
<th>FUNCTIONAL AREA</th>
<th>RECOMMENDATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requirements</td>
<td>Ensure requirements allow for flexibility</td>
</tr>
<tr>
<td>Contracts</td>
<td>Dynamic enough to align with technological changes</td>
</tr>
<tr>
<td>Funding</td>
<td>Be sure funding is flexible enough to align with technological changes (BA-08 Pilot)</td>
</tr>
</tbody>
</table>

### 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.

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

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

IT Box Framework (5 years)

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

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
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
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

Defensive Cyber Operations (DCO) is a set of strategies and techniques designed to protect computer systems and networks from cyber threats. It involves a range of tools and methodologies to detect, deter, and respond to cyber attacks.

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


### Platforms and Development

- **Garrison DCO Platform (GDP) (FIXED):** Supports mission planning and situational awareness for Cyber Wargaming, Analyses, Training, Network Visualization. Coordinates with Joint solution for increased efficiencies and shared capabilities.

- **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.

- **DCO Development Environment (DCODE):** Innovation and Deployment, Forge (Develop), Armories (Deploy), Development Environment (Training, Testing and Integration).

### 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.

### Defensive Cyberspace Operations Tools Suite

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

**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.

### DCO Mission Planning (DCOMP)

**Supports mission planning and situational awareness for Cyber Wargaming, Analyses, Training, Network Visualization.**

### User Activity Monitoring (UAM)

- Identifies and malicious activity.
- Monitors Insider Threat for SIPRNet, JWICS, SAP.

### 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;
- Develop intelligence.
### Future Requirements

Please view our upcoming procurement forecast and opportunities here: [https://www.eis.army.mil/opportunities](https://www.eis.army.mil/opportunities)  
[https://vulcan-soft.com](https://vulcan-soft.com)

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