Defensive Cyber Operations (DCO) provides operational capabilities in order to defend our nation’s networks. Defensive cyber functions in a Development and Operations (DevOps) environment allowing for stakeholder collaboration and software integration. We provide improved prototype frequency, rapid product delivery to our cyber defenders, ultimately delivering a lower failure rate on tools development. Improved collaboration and communication between organizational teams and industry enables us to achieve faster prototyping and delivery to our global cyber defenders.

**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.

**VISION**
Be recognized as the leader within the cyberspace domain delivering innovative, integrated and cost effective solutions.
Defensive Cyber Operations (DCO) Overview

**HOW WE SUPPORT OUR SOLDIERS**

- Provide 10 Acquisition Category (ACAT) III and IV Programs of Record
- 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 and Intelligence (C4I) acquisition services

### Other Capabilities

<table>
<thead>
<tr>
<th>Cyber Analytics and Detection (CAD)</th>
<th>Cyber Platform and Systems (CPS)</th>
<th>Applied Cyber Technologies (ACT)</th>
<th>Technology Applications Office (TAO)</th>
<th>Allied Information Technology (AIT)</th>
</tr>
</thead>
<tbody>
<tr>
<td>· Cyber Analytics (CA)</td>
<td>· Defensive Cyber Operations Tools Suite (DCO Tools Suite)</td>
<td>· Forge and Armory</td>
<td>· Functionally integrated, task force organization designed to provide centralized, life-cycle management</td>
<td></td>
</tr>
<tr>
<td>· User Activity Monitoring (UAM)</td>
<td>· Deployable Defensive Cyberspace Operations Systems – Modular (DDS-M)</td>
<td>· Continual Integration</td>
<td>· Engineering, fielding, and operation of IT and infrastructure projects, supporting programs</td>
<td></td>
</tr>
<tr>
<td>· Castle Keep</td>
<td>· Garrison Defensive Cyberspace Operations Platform (GDP)</td>
<td>· Upgrade/Test Capabilities</td>
<td>· U.S. and Partner Nation Security and Interoperability, Non-Standard IT Solutions</td>
<td></td>
</tr>
<tr>
<td>· Defensive Cyber Operations Mission Planning (DCOMP)</td>
<td>· Forensics and Malware</td>
<td>· Anytime Training</td>
<td>· Foreign Military Sales Lifecycle</td>
<td></td>
</tr>
<tr>
<td>· Threat Emulation</td>
<td>· Advanced Sensors</td>
<td>· One-Stop Shop Capabilities</td>
<td>· Technology Transfer</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>· Capability Optimization</td>
<td>· Acquisition</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>· Soldier Operational Environment</td>
<td>· Foreign Policy Review and Oversight</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>· Development, Security and Operations (DevSecOps) Model</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

• Provide rapid prototyping capabilities for rapid acquisition
• Foreign military sales - building partner relationships
• Command, Control, Communications and Intelligence (C4I) acquisition services
Defensive Cyber Operations (DCO) Major Accomplishments in 2020

- Successfully delivered Deployable Defensive Cyberspace – Modular (DDS-M) kits to the warfighter, and provided over 10 Net Equipment training classes to our cyber defenders.
- Successfully worked with ARCYBER, Intel Community, and ACC-RI to add the JWICS capability to the Army’s Big Data Platform (BDP); Awarded contract to enhance critically needed teleconference capabilities (via GN Chat) to more than 900+ users during the COVID-19 pandemic.
- Established Forge/Armory interconnected multi-site environment to deliver DCO capabilities and tools to our cyber defenders.
Cyber Analytics and Detection (CAD) focuses on programs that are software-based which supports mission command, planning, integration, analysis, and execution at all levels. Our capabilities integrate cybersecurity requirements, intel & vulnerability analyses with the outputs of mission analysis to determine probable attack vectors and produce internal defense measures. Our programs offer interfaces and visualizations accessible by cyberspace defenders at all levels to facilitate counter-reconnaissance activities meant to discover the presence of advanced or sophisticated cyber threats and vulnerabilities.

Lieutenant Colonel Leilani Tydingco-Amarante
Product Manager
Defensive Cyber Operations (DCO)
Cyber Analytics and Detection (CAD)

Cyberspace Analytics:
Main capability is the Army's Big Data Platform (BDP) -- Gabriel Nimbus. Based on DISA's Big Data Platform. Distributed Queries support missions outside of DCO, allowing for rapid identification and mitigation of threats. Eliminates the use of manual searches. Receives data via batch files and transfers arrive hourly. System ingests data and capable of sharing this data with other BDP instances.

UAM:

Castle Keep:
Monitor Army SCIFs. Work with Army G-2.

DCOMP:
Mission planning and synchronization software. Transition of DARPA PlanX to PhalanX to DCOMP Solution. Currently testing the first capability drop providing users with C2Core, Battlespace Analytics, Battlespace Viewer, ThunderRidge, Pathfinder & ENVE enriched data feed. Applications will reside on the BDP and can be deployed on a kit.

Threat Emulation:
DCO and operational focused. Operational training through battle drills. Decreases time to detect, time to identify and time to respond. Uses existing DCO maneuver platforms to assess people, processes and systems' ability to withstand threats.
Cyber Platform and 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. Defensive Cyberspace Operations Tools Suite (DCO Tools Suite) provides industry’s best capabilities to the warfighter. These tools are used on the cyber platform to effectively conduct their cyber protection team missions.
Defensive Cyber Operations (DCO)  
Cyber Platforms and Systems (CPS)

**Deployable Defensive Cyberspace Operations Systems-Modular (DDS-M)**
Is a configurable hardware kit that can be easily transported by aircraft and other means of transportation. It is armed with the ability to tap into a network and host tools for defensive measures.

**Garrison Defensive Cyberspace Operations Platform (GDP)**
Provides remote operational capability and a common platform opportunities between DCO and Department of Defense Information Network-Army (DoDIN-Army) systems. It has the ability to integrate with Cloud, GN, and GEF

**Defensive Cyberspace Operations Tools Suite (DCO Tools Suite)**
Integrates 32+ Commercial Off-the-Shelf (COTS) and open-source software (OSS) tools and products and continually leverages the user assessment approach
- Drives investment and divestment
- Validates enduring effectiveness

**Forensics and Malware Analysis (FM&A)**
Forensics and Malware Analysis team 90 day priority is to begin the process of delivering the EnCase Investigator capabilities to the Regional Cyber Commands (RCCs) and to visit the Department of Defense Cyber Crime Center (DC3) Forensics Lab teams to discuss their tools being used to support Forensics and Malware.
APPLIED CYBER TECHNOLOGIES (ACT)

Applied Cyber Technologies (ACT) through DCO Development Environment (DCODE), is the mechanism to bring in rapid innovation, sustainment of Defensive Cyber Systems, and Training and DEVSECOPS Environment. This capability spans three mission sets: Forge, Armory and Mission network. The Forge brings innovation to the Army through rapid defensive cyber capability prototype development. Using the Cyber Operations Broad Responsive Agreement (COBRA) Other Transaction Agreement (OTA), it develops prototypes by leveraging industry expertise and partnerships. The Armory is where DCO Suite of Complimentary Systems (DSCS) are housed and sustained. This allows Cyber Protection Leadership to quickly ensure kits are always mission ready. The Mission Network infrastructure enables maneuver and collaboration with operational forces allowing them to leverage remote mission support services and collaboration with industry and academia.

Lieutenant Colonel Peter Amara
Product Lead
Defensive Cyber Operations (DCO) and Applied Cyber Technologies (ACT)

**Forge**
- Process initiated by technology, security, warfighter, and other requirements
- Input solicited from vendors, academia, and government for solutions to requirements
- Evaluation and assessment is in a closed, controlled environment on virtualized infrastructure of common services, tools, and/or platforms
- Output consists of packages with test and evaluation metrics for each product, software and/or hardware, licensing, documentation and training

**Armory**
- Forward deployed facility to support the Warfighter in optimizing current systems and capabilities, and to improve operational effectiveness and efficiency
- Repository contains software, updates, patches, licensing, training and programs of record
- Mechanism to identify and assess issues, conduct performance analysis and provide continuous feedback
- Mission-focused training using the latest integrated capabilities

**DCO Development Environment (DCODE) Network**
- Infrastructure that enables maneuver and collaboration with operational forces
- Allows cyber defenders to leverage remote mission support services and collaboration with industry and academia
Defensive Cyber Operations
Upcoming Opportunities/ Needs from Industry

- Forensics and Malware Analysis (F&MA) – Licences, Training, Professional Services and Maintenance
- Deployable Defensive Cyberspace Operations – Modular, New Equipment Training Virtualization
- Cloud Based Garrison Defense
- Allied Information Technology has 11 Letters of Request (LOR), 23 cases in development, and 23 active cases

**BEHAVIORS NEEDED**
- Be Innovative
- Be A Participant, Get In The Game
- Integrate With Each Other
- Be Flexible
- Be A Team Player
- Provide Metrics That Demonstrate Your Value

**CAPABILITIES NEEDED**
- Network Mapping
- Counter Infiltration Tools
- Cyber Intelligence Integration
- Data Analytics – Artificial Intelligence and Machine Learning
- Security Orchestration, Automation and Response (SOAR)
- Threat Analysis
# Defensive Cyber Operations (DCO) Opportunities

<table>
<thead>
<tr>
<th>PM/PD/PL</th>
<th>Description</th>
<th>Contract Office</th>
<th>Vehicle Contract or Method</th>
<th>Quarter &amp; FY of Solicitation</th>
<th>Estimated Award Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>DCO</td>
<td>DCO SETA-Re-compete</td>
<td>TBD</td>
<td>TBD</td>
<td>TBD</td>
<td>Q2 2021</td>
</tr>
<tr>
<td>DCO</td>
<td>DCO Laptop Refresh</td>
<td>ACC-RI</td>
<td>TBD</td>
<td>TBD</td>
<td>Q2 2021</td>
</tr>
</tbody>
</table>