Start your Career as an Army Professional at the U.S. Army Cyber Command!

The mission of the U.S. Army Cyber Command’s (ARCYBER) Career Exploration, Advancement and Development (CEAD) Program is to build a highly competent pipeline of cyber professionals to expertly perform and adapt to an ever-changing cyber operational environment. Working as an Army Civilian Professional offers highly technical individuals a rare chance to challenge their skills on world-class national defense problems. Army Civilians are an integral part of the Army team, who are committed to selfless service in support of the protection and preservation of the United States.

As an Army Civilian Professional, you can serve your country and support your military counterparts by using your technical expertise to make an impact on Soldier capabilities, support overseas operations and disaster relief projects, and develop technology systems and capabilities that give a technological advantages to the nation’s warriors. In cyberspace your technical skills will be valued and engaged every day in defense of the nation.

You will work right alongside uniformed military counterparts, receive hands-on training, education, and have access to certificate programs and professional and leadership development opportunities as you progress throughout your career. ARCYBER has short-term (10 weeks) internships and long-term (2 years) fellowships available.

About Army Engineers and Scientists
With the need for everything from biologists to computer programmers, and mathematicians, the Army’s mission offers an unparalleled range of career opportunities and experiences for civilian engineers and scientists (non-construction) in Computers; Software; Electrical; and Operations Research fields.

About Army Cyber Needs
The rise of cybersecurity threats has placed unprecedented demands on IT/Cyber professionals to quickly learn new competencies and perform in turbulent environments. Join the cadre of software, hardware and tool developers, electrical engineers, programmers and coders, mathematicians, network and cloud technicians, data and malware analysts, technical writers, budget analysts, and many more technical professionals on the Army Cyber team.

Locations Worldwide
Within ARCYBER, more than 16,500 military, civilian and contract personnel work across the globe. Explore the world and work for an organization that will provide more than a pay check, but a purpose, mission, and a way to contribute to your country while developing professionally.
CEAD Program Vitals

Mission: To build a highly competent team of cyber professionals to expertly perform and adapt to an ever-changing cyber operational environment.

Purpose: To meet strategic human capital needs of the Command and grow the workforce.

Participants: The program seeks cyber experts to join the ranks of the ARCYBER team. Candidates may be current high school and college students studying cyber fields, recent graduates, seasoned technology professionals interested in a career with ARCYBER.

Skills Sought include but not limited to: Computer, electrical and software engineering, programming, coding, mathematics, cloud computing, digital/computer forensics; data analysts/scientists, malware analysis, computer science, budget, knowledge management, technical writing.

Army Cyber Command CEAD Program Overview

The ARCYBER Career Exploration, Advancement, and Development (CEAD) Program is a command-wide initiative comprised of short-term internships and long-term fellowships for cyber professionals. The program offers on-the-job training, projects, rotation assignments, and other training. Participating organizations include: ARCYBER, U.S. Army Network Enterprise Technology Command (NETCOM) Cyber Protection Brigade and Regional Cyber Centers (RCCs), the U.S. Army Intelligence Command’s 780th Military Intelligence Brigade, and the Joint Force Headquarters-Cyber.

The CEAD Program is designed to deliver a team of cyber professionals who expertly perform and adapt to an ever-changing cyber operational environment. The program provides experiential-based training anchored on a 4-point training strategy that includes academics, leadership training, broadening experiences and technical training events. The CEAD Program fosters diverse experiences to increase the aptitude for success and dominance within the cyberspace domain. Upon acceptance into the program, participants work as full-time employees and are required to obtain a top secret/secret compartmented information security clearance. Entry-level pay grades are based on education and experience. There are opportunities for non-cyber fields to include budget/finance, English, technical writing and more.

Short-term Internship Program (10 weeks)

Rising high school and college juniors and seniors may apply to paid short-term summer internship opportunities to work for the Command prior to graduation. ARCYBER utilizes several programs to recruit cyber talent. Army Pathways Summer Interns are current students in high school, college, trade schools and other qualifying educational institutions. Additionally, ARCYBER supports the following Department of Defense (DoD) Scholars programs: Cyber Talent Initiative; CyberCorps® Scholarship for Service (SFS) Program; Cyber Scholarship Program (CySP); and the Science, Mathematics, and
Research for Transformation (SMART) Program. A student does not have to belong to any of the aforementioned programs to be considered for a short-term internship. Program features include:

- Intern Orientation
- On-the-job training and problem-based projects
- Functional training and senior leader engagements
- Potential part-time work opportunities during the school year

**Long-term Fellowship Program (2 Years)**

The CEAD Long-term Fellowship Program provides an entry option for recent graduates and exceptional cyber talent without degrees. Fellows are hired into developmental positions and may be promoted each year of the program, pending performance and supervisor approval. Fellows may be required to commit to a continued service agreement, adhere to a mobility agreement, and must complete the program’s training plan. CEAD Fellows may be hired as – but not limited to - Army Pathways Recent Graduates, using the Cyber Direct Hiring Authority, DoD Cyber Scholar graduates; or programs such as the DoD Cyber Talent Initiative. Program features include:

- On-the-Job Training, Technical Training, and Project-Based Assignments
- Rotational Assignments and Interagency Visits
- Leadership Training and Senior Leader Engagements
- Civilian and Military Mentorship Opportunities
# U.S. Army Cyber Command (ARCYBER)
## Career Exploration, Advancement, and Development Program

**We are seeking YOUR skills!**

<table>
<thead>
<tr>
<th>ARCYBER</th>
<th>NETCOM</th>
<th>CPB</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mission</strong></td>
<td>The U.S. Army Network Enterprise Technology Command (NETCOM) leads global operations for the Army’s portion of the Department of Defense Information Network, ensuring freedom of action in cyberspace while denying the same to our adversaries.</td>
<td>The Cyber Protection Brigade defends <strong>key terrain</strong> against <strong>specified threats</strong> to deliver effects that ensure freedom of action in and through cyberspace and to deny the same to our adversaries.</td>
</tr>
<tr>
<td><strong>Locations</strong></td>
<td>Fort Huachuca, AZ; Fort Gordon, GA; Fort Bliss, TX; Fort Bragg, NC; Fort Carson, CO; Fort Detrick, MD; Fort Drum, NY; Fort Eustis, VA; Fort Hood, TX; Fort Leonard Wood, MO; Fort Myer, VA; Joint Base San Antonio, TX; Joint Base Lewis-McChord, WA; Redstone Arsenal, AL; Fort Sill, OK; Fort Meade, MD; Wiesbaden, Germany; Korea; Japan</td>
<td>Fort Huachuca, AZ; Fort Gordon, GA; Fort Meade, MD</td>
</tr>
<tr>
<td>Fort Belvoir, VA; Fort Gordon, GA; Fort Meade, MD*</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*In 2020, ARCYBER will relocate to Fort Gordon, GA*
# U.S. Army Cyber Command (ARCYBER) Career Exploration, Advancement, and Development Program

## Training Tracks

<table>
<thead>
<tr>
<th>Information Technology Management:</th>
<th>Engineering:</th>
<th>Engineering:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customer Service;</td>
<td>Computer; Software; Electrical; Operations Research</td>
<td>Computer; Software; Electrical; Operations Research</td>
</tr>
<tr>
<td>Information Security;</td>
<td>Information Technology Management:</td>
<td>Information Technology Management:</td>
</tr>
<tr>
<td>Systems Analysts;</td>
<td>Customer Service; Information Security; Systems Analysts; Network; Policy and Plans</td>
<td>Customer Service; Information Security; Systems Analysts; Network; Policy and Plans</td>
</tr>
<tr>
<td>Network; Policy and Plans</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Projects

<table>
<thead>
<tr>
<th>- Cloud On-Premise, Off-Premise and Hybrid technologies</th>
<th>- Engineer a modern, integrated, and operational network; centralize management of enterprise networks and systems.</th>
<th>- Computer Science and Data Science work role efforts within the brigade.</th>
</tr>
</thead>
<tbody>
<tr>
<td>- File Migration and DCO/SAN build out</td>
<td>- Execute strong compliance and inspection programs.</td>
<td>- Analytic pipeline training development.</td>
</tr>
<tr>
<td>- Future Operations</td>
<td>- Enable strategic and tactical mission command.</td>
<td>- Analytic inventory research and development.</td>
</tr>
<tr>
<td>- Microsoft Project Server</td>
<td>- Refine operate/maintain/defend network requirements.</td>
<td>- Big data platform research and support to operational teams.</td>
</tr>
<tr>
<td>- Disaster Recovery Planning</td>
<td>- Improve emergency and network services.</td>
<td>- Reduce cyber-attack surface, improve network defense.</td>
</tr>
<tr>
<td></td>
<td>- Prioritize network modernization effort and maintenance.</td>
<td></td>
</tr>
</tbody>
</table>

---

We are looking for both short-term interns and long-term fellows working full-time in a developmental capacity in a variety of offices.

Summer interns may onboard annually May – June. Typical short-term internship length is 10 weeks. Long-term fellowships are typically 2 years, onboard dates may vary. Transcripts are required. Unofficial transcripts are acceptable. **Please forward a copy of your most current resume and transcripts to:** usarmy.belvoir.arcyber.mbx.internships@mail.mil. Indicate if you are interested in a short-term, long-term internship or both and your area of interest.

**Eligibility Requirements:**

Must be a Scholarship for Service (SFS) recipient; U.S. Citizenship is required; Pre-employment drug testing is required; and Ability to obtain and maintain a Top Secret/SCI security clearance.
ARCYBER Chief Information Officer/G6 Internship

Short-term Internships (10) weeks

Short-term interns will be assigned to the Cybersecurity Programs Division where they will research, develop and update Cybersecurity policies. Interns will participate in projects and apply the Risk Management Framework (RMF) process throughout the system development life-cycle, to include requirements definition, analysis, design/architecture, development, and testing for new systems or major enhancements to existing systems. Participants will also gain experience in managing software based systems, which impacts the organization worldwide. Interns will come onboard as Information Technology Management Specialists at the GS-03, 04 or 05 levels depending on experience and education qualifications.

Interns will develop knowledge, skills and abilities in the following areas:

a) **Leadership Skills**: Ability to interact with a team to gain understanding of web applications, answer technical queries, and make recommendations on documentation to ensure professional presentation.

b) **Oral Communication**: Routinely deliver information, tailored to audience (for example, technical, sensitive, controversial); make clear and convincing oral presentations; listen to others while interpreting nonverbal cues, and respond appropriately.

c) **Problem Solving**: Identify and deconstruct problems; determine accuracy and relevance of information; use sound judgment to generate and evaluate alternatives, and make recommendations.
Long-term (2-year) Fellowships

ARCYBER’s CIO/G6 long-term fellowship experience is an expansion of the short-term program, typically lasting for 2 years. Our fellows help maintain and defend the Army’s Network while working full-time as Information Technology Management Specialists. In this role, fellows gain experience in written and oral communication, presentation, problem solving skills. The program, follows a master training plan that addresses core skills such as communications, writing, business and time management skills presentation skills and leader development as well as specialized technical skills in customer service, information security, systems analysis, network, and policy and plans. This program consists of rotational assignments in locations across the globe.

Fellows join the ARCYBER team as Information Technology Management Specialists at the GS-07/09/11 levels depending on experience and education qualifications with permanent placement opportunities. Job duties may include:

a. **Information Security**: Conduct risk and vulnerability assessments of planned and installed information systems to identify vulnerabilities, risks, and protection needs. Assess security events to determine impact and implement corrective actions. Installs, configures and supports cyber security tools such as Security Onion, McAfee Host Based Security Suite (HBSS), Assured Compliance Assessment Solution (ACAS), Security Event and Incident Management (SEIM). Recognizes security events and takes appropriate action to identify threats and implement countermeasures.

b. **Systems Analysts**: Perform network traffic analytics to identify threats. Audits logs looking for anomalous actions and possible insider threats. Surveys and evaluates network traffic and creates network diagrams.

c. **Policy and Plans**: Develop policies and procedures to ensure information systems reliability, accessibility and ability prevent and defend against unauthorized access to systems, networks and data. Conduct systems security evaluations, audits, and reviews.

d. **Network**: Network and systems design to ensure compliance with systems security policies. Ensures network security and triage resolutions. Performs computer network defense (CND) incident response.

e. **Customer Service**: Using effective communication skills, serve on the help desk fielding queries from users from across the organization to resolve network and system issues.