



U.S. ARMY

# Cyber Branch

## Talent Priorities

Year Group 2019



**INTELLIGENCES:** Logical-Mathematical, Spatial, Interpersonal

**SKILLS:** Cyber Corps officers are innovative, adaptive, resilient, and intellectually curious leaders, capable of applying the art and science of the profession of arms within the cyberspace warfighting domain and electromagnetic spectrum (EMS), leading offensive and defensive cyberspace operations and electronic warfare (EW) actions. They must be technically superior and passionate, understanding the cyberspace domain and EMS in a multi-dimensional sense to leverage leading-edge technologies and technically-skilled teams to provide operational commanders a unique effects-based capability for defending our nation against emerging cyber threats. They must effectively articulate cyberspace and EW operational capabilities to commanders, as well as, integrate those capabilities to create effects in unified land operations across joint, interagency, intergovernmental, and multinational environments. They must also be lifelong learners to continue developing expertise as leaders in their field and be highly adaptive within an emerging technological environment.

**KNOWLEDGE:** The Cyber Corps highly values officers with academic backgrounds in specific Science, Technology, Engineering, and Mathematics (STEM) disciplines and majors, but not exclusively. The domain-specific education disciplines listed below provide officers with a greater level of knowledge needed to plan, synchronize, and lead cyberspace operations. Other STEM and liberal arts disciplines and majors are also valued, but should be accompanied with demonstrated, cyber-related technical aptitude.

- **RELEVANT EDUCATION:** Computer Science; Computer Engineering; Computer Information Systems; Cyber Security/Operations; Data Science; Electrical Engineering; Information Technology/Systems Security; Mathematical Sciences; Mechanical Engineering; Physics/Chemistry
- **RELEVANT TRAINING / EXPERIENCE:** Cyber Leader Development Program (CLDP); Cadet Troop Leading Time / Cadet Leader Development Time (CTLT / CLDT) with cyber-related units; capture the flag events (team and individual); industry / hacking conference participation; globally-recognized cyber-focused certifications; academic enrichment programs or internships with higher education, research, private sector, or government agencies.

**BEHAVIORS:** (In addition to foundational)

- |                 |                       |               |               |                   |
|-----------------|-----------------------|---------------|---------------|-------------------|
| ➤ AGILE         | ➤ CRITICALLY THINKING | ➤ DISCIPLINED | ➤ INQUISITIVE | ➤ PROBLEM SOLVING |
| ➤ AMBITIOUS     | ➤ DETAIL FOCUSED      | ➤ EXPERT      | ➤ PASSIONATE  | ➤ RATIONAL        |
| ➤ COLLABORATIVE | ➤ DILIGENT            | ➤ INITIATIVE  | ➤ PERCEPTIVE  | ➤ RESILIENT       |
| ➤ CONFIDENT     | ➤ DIRECTIVE           | ➤ INNOVATIVE  | ➤ PRECISE     | ➤ VISIONARY       |

**TALENT PRIORITIES:**

1. **PROBLEM SOLVER:** Able to choose between best practices and unorthodox approaches to reach a solution. Accomplishes the task.
2. **DOMAIN-SPECIFIC EDUCATION:** Possesses relevant academic disciplines desired by specific branch.
3. **INNOVATIVE:** Creative, inquisitive, and insightful. Easily identifies new solutions and catalyzes change.
4. **INSPIRATIONAL LEADER:** Motivates teams to work harmoniously and productively towards a common goal.
5. **TECHNOLOGICALLY ADEPT:** Understands and effectively uses the latest technologies.
6. **LOGICAL / ANALYTICAL:** Uses reason and thinks in terms of cause and effect. Able to deconstruct and solve complex problems.





U.S. ARMY

# Minimum Requirements



- Must be a U.S. citizen.
- Must obtain and maintain a TOP SECRET clearance.
- Must receive a favorable special background investigation with eligibility for sensitive compartmented information.
- Must be able to pass a counter-intelligence scope polygraph (unit/assignment based).
- Bachelor's of Science or higher degree in specific STEM disciplines preferred, but not required.
- Must successfully complete the Cyber Branch assessment and selection process, which includes but is not limited to an interview, aptitude assessment, written questionnaire, and supporting documents packet review.





U.S. ARMY

# Cyber Branch Assessment & Selection Packet

## for Qualified OCS Candidates



### Checklist:

- Completed Cyber Branch Questionnaire (available at OCS or from Office, Chief of Cyber)
- Letters of Recommendation (from OCS packet acceptable)
- College Transcript(s) (unofficial copy acceptable)
- Civilian Resume (if not providing a military record document)
- Enlisted Record Brief (or similar military record, if applicable)
- Notification of Acceptance to OCS (for applicants who are not currently in the service.)
- Copy of the OCS essay (from OCS packet)
- Copies of cyber-related certifications and/or training certificates or transcripts (e.g. CompTIA, ICS<sup>2</sup>, EC-Council, ADET/NCS)

INSTRUCTIONS: Submit documents in the order listed above in one file, or in as few files as possible, to the Office of the Chief of Cyber's Officer Division at: [usarmy.gordon.cyber-coe.mbx.occ-officers@mail.mil](mailto:usarmy.gordon.cyber-coe.mbx.occ-officers@mail.mil). Following receipt and assessment of packets, phone interviews will be scheduled in most cases before a selection determination is reached and notification is made.

