

Cyber Protection Team 173/ Defensive Cyber Operations Element Assessment and Selection FAQ

A&S

This Assessment and Selection process is for M-Day positions.

-We do have opportunities to do TDY/ADOS tours of varying lengths throughout the year. However, even these opportunities are not guaranteed. Most members of the team hold full time employment positions in civilian organizations.

-CPT 173 and the DCO-E can only accept New York Army National Guard (NYARNG) members. If you are a member of another state or component, any acceptance to the team is tentative pending your transfer (both inter-state and/or component). Excessive delays may cause any acceptance to be rescinded. Service Members of other components **MUST to talk with an NYARNG recruiter to ensure they understand the requirements and process to join.**

-NYANG members: Both ANG Wings in New York have Mission Defense Teams (MDT's), which is their inward focused cyber element.

-Civilians, ROTC/OCS, and applicants from other components must talk to a recruiter first. Express your interest, get started with the recruitment process, and have them contact us to discuss opportunities. Generally, we will not accept packets until a candidate is medically cleared and has received their ASVAB scores.

Packet Submission

- **What is the timeline for the FY25 assessment and selection?** Applicants will need to submit packets prior to 3 JAN 2025. Any applications received after this will be rolled to the next FY. Applications can be sent to ng.ny.nyarng.mbx.cyber-recruiting@army.mil. By 1 February 2025, notifications will be sent for those that passed or did not pass the resume review. Those that pass the review will be invited to attend the in-person assessment and selection at the Kingston Armory, (Date TBD) FEB 2025. If any dates or location change, notifications will be sent to all applicants. Exceptions to the in-person portion may be granted.
- **What documents do I need to submit?**

At minimum, all applicants must submit a civilian resume and official document with ASVAB scores.

- For current Army Service Members: ERB/SRB (ASVAB and PULHES scores must be visible) or ORB.
- For current Service Members of other components: Please speak to a recruiter. We will answer any questions on an individual basis.

- Failure to provide either required document by the end of the submission period will result in non-selection during packet review.
- **Once I submit my packet, can I add to it?** Yes! Your packet is not an immutable object. You can add to and update documents after submission as you gain additional credentials, work on projects, change jobs, and continue to gain experience. Simply send any new or updated docs to the same recruiting email and we will add them to your packet.

Packet review

1. **Does submitting my resume and ERB/ORB mean I will go through the Assessment and Selection?** No. The leadership will review each “packet”. Common reasons for initial non-selection include:

- Not meeting the minimum ASVAB scores (both GT and ST). This is a hard requirement and NGB will not accept ASVAB waivers.

For enlisted applicants, the minimum score for General Technical (GT) is 110 **AND** Minimum score for Skilled Technical (ST)-112/114/116 depending on the date you took your ASVAB (see the table below).

| ASVAB date | GT min score | ST min score |
|-----------------------------------|--------------|--------------|
| After 1 APR 2014 | 110 | 112 |
| Between 2 JAN 2002 and 1 APR 2014 | 110 | 114 |
| Before 2 JAN 2002 | 110 | 116 |

For warrant officer applicants/candidates, please see the requirements at <https://recruiting.army.mil/ISO/AWOR/170A/>

- Lack of desired skills, knowledge, experience, or potential. This is not to say that if you are new to cyber security, you do not have a chance. The leadership takes a very holistic view of each applicant to decide if the applicant will be an asset to the team. This is balanced against what the team needs.
- PULHES. Requirement is a min of 222221 (this is on your ERB/ORB). Again, this is a hard requirement and NGB will not entertain a waiver. Any 3’s on your PULHES MUST be addressed before any acceptance will be offered.

Assessment and Selection event

- **What does the assessment entail?** This is an in-person interview and hands on capture the flag style assessment of your understanding and knowledge/ability in cybersecurity, OSINT, networking, incident response, forensics, Linux, windows, cyber mission force structure/organization and other areas.
- **What is the interview?** Similar to a board/job interview but done informally. This is a 30–45-minute snapshot of you.
-

Determination

- **Will applicants be notified if they are non-select and the reason?** Yes, anyone not selected will be notified and an explanation of the reason given via email.
- **Once the AnS is complete, how soon will I know if I am selected?** Generally, we will notify the applicant of acceptance or rejection within 30 days following the interviews.
- **What do I need to do if I am accepted?** You need to work with your current Chain of Command to begin the process to be attached to CPT 173/DCO-E. For those that are accepted from another State, you will need to start the IST process. During this time, the majority of the work is on you. We will assist where possible but maintaining good relations with the losing unit is critical. NCOER/OER/awards **must** be completed prior, along with any hand received items or equipment turn-in. Keep the full-time staff apprised of your progress and if you run into any hurdles.
- **What happens if I am not selected?** Same as #4, we will notify you with the reason. We encourage all who are non-select to improve their skills and gain further experience.
- **If I am accepted and transfer, then what is next?**
 - We will work with you on the process to become a 17A (Officer), 170A (Warrant Officer), 17C (Enlisted) or 35F (Enlisted). These are the only positions on the team. This can entail going to a reclassification school(s) or submission of a reclassification packet and identifying additional required training that you must complete.
 - New members will be in a probation (attached to the unit, not assigned) status with another member of the team placed in a mentoring status over them. The mentor will “guide” the new member through much of the follow-on requirements. Failure to show progress can result in negative actions to include removal from the team.
 - There is also the expectation that you will stay with the team for an extended period. We invest a lot of time and effort into each member of the team and expect a return on that investment. Obviously, Officers are slightly different due to how the State manages those slots.
- **How long does all this additional training take?** 1-3 years depending on the MOS and work role requirements. Prior experience, training and certifications can reduce this time.
- **What happens if I fail or do not pass some of the training?** Depending on the item, this can result in removal from the team. Failure of a MOS/branch producing school will most likely result in removal.

General Information:

- **How many positions and what ranks are you looking to fill?** We do not recruit to fill a vacancy. We recruit talent. If none of the applicants meet our standards, then none are selected. We will attempt to put candidates in contact with other units if positions are not available with us.
- **Clearance Requirements.** You must be able to obtain a fully adjudicated TS/SCI clearance and pass a counterintelligence polygraph.

Team information

- **Where do you drill?** Kingston, NY.
 - **What are ATs like?** For most on the team, AT will be attendance at a National or regional cyber exercise.
 - **What are drills like?** Usually this is prep for the next large exercise, hands on training, administrative actions (NCOER/OER/awards), better refining our procedures, and mandatory training. Even though we are a Cyber unit, we still must meet the normal Military requirements.
 - **Will I have the opportunity for promotions?** Maybe. Since members are usually pulled to the unit at the mid-point in their career, advancement is competitive after E6/O3. We have very limited Field Grade and Sr Enlisted positions. Warrants can advance to W4. The team supports both enlisted and officers to pursue WO.
 - **Do you mobilize?** Yes, mobilizations are expected to be about 14 months.
 - **What's the difference between the CPT and DCO-E?** The CPT is a deployable unit that is geared towards incident response outside of DoDIN. The DCO-E is geared towards incident response on DoDIN. Both units train and drill together and have the same requirements.
 - **What else should I expect being on the CPT/DCO-E?** We expect all members to continuously improve and build their skills. The unit requires training events outside of the traditional one weekend a month / 2 weeks a year. All current members work within the Cyber/Intel/IT Community in some capacity. This is a team of experts; either in cyber defense, cyber management/operations, forensics, network defense and hardening, architecture, malware analysis and other areas. Members are expected to be extremely proficient and able to operate/function with little guidance.
 - **Do you 'go to the field'?** Not usually. We do, in rare instance, send team members to support maneuver units. However, expect operations to take place in an office environment.
 - **Are there ADOS / SAD opportunities?** Yes, we do put Soldier's on ADOS orders for specific events. With that being said, this is NOT a unit that simply supports members riding the orders money train. If you're on orders, you're going to work.
1. **How much time requirements are expected outside of drill?** More than most other units, but we are reasonable and do work to compensate Soldier's for that.
 2. **Is being on the team hard?** Compared to most other units, yes. Members have very high expectations and requirements placed on them. This is balanced against the rewards of very specialized training, incentives, and an excellent network of others to assist if you want to work in the cyber security sector on the civilian side. Unlike traditional Units, members are expected to continue training on their own between drills, maintain active communication with the unit throughout the month, and participate in response missions.