

Appointment Letter Template (CNDSP)

Date (MM/DD/YYYY)

Major Command

Office Symbol

Sub Organization

MEMORANDUM FOR RECORD

SUBJECT: Designation of Cybersecurity (CS) Support Personnel

1. References: AR 25-2 Chapter 3 and DoD 8570.01-M.
2. Effective immediately, the below individual is appointed to perform Cybersecurity duties and functions for the category and level below.

Full name

Duty position/role

AKO or EE mail address

Civilian series/
MOS

Personnel
Category

IT Position Category

Supervisor AKO/EE mail address/phone
number

Contract #/Expiration date

IT Support Services

CYBERSECURITY CATEGORY AND LEVEL

Primary Duty

Additional/Embedded

3. Purpose: To perform Cybersecurity functions and duties IAW the DoD 8570.01M category and level listed above.
4. Period: Until officially relieved or released from appointment, or upon transfer, termination, reassignment, retirement or discharge.
5. Special instructions:
 - a. Register in the Army Training and Certification Tracking System (<https://atc.us.army.mil>).
 - b. Complete required IA training and certification for category/level. Review the IA Training and Certification BBP.
 - c. Complete and sign Privileged Access Agreement (PAA)/Non-Disclosure Agreement and Acceptable Use Policy then upload in ATCTS.
 - d. Ensure the DD 2875 is signed in part IV by the servicing Network Enterprise Center/Service Provider noting elevated privileges are approved/denied.
6. Soldiers annotated as 25B/25U w/supervised access will sign a PAA and work under the direct supervision of an IATI or higher baseline certified DA civilian or military individual. They will be designated as 25B/25U w/ supervised access in ATCTS and meet the Computing Environment certification or certificate of training requirement per DoD 8570.01-M. Personnel in this category are not authorized certification vouchers from Army CIO/G6 voucher program.

Name of commander or designee
signing letter

Position/Role

Grade

Signature

Functions/responsibilities-Check all that apply

Receive and analyze network alerts from various sources within the NE or enclave and determine possible causes of such alerts.

Coordinate with enclave CND staff to validate network alerts.

Recommend, schedule, and/or implement IA related repairs within the enclave environment.

Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.

Monitor external data sources (e.g. CND vendor sites, Computer Emergency Response Teams, SANS, Security Focus) to maintain currency of CND threat condition and determine which security issues may have an impact on the NE or enclave.

Assist in the construction of signatures which can be implemented on CND network tools in response to new or observed threats within the NE or enclave.

Perform event correlation using information gathered from a variety of sources within the NE or enclave to gain situational awareness and determine the effectiveness of an observed attack.

Notify CND managers, CND incident responders, and other CND-SP team members of suspected CND incidents and articulate the event's history, status, and potential impact for further action.

Create, edit, and manage changes to network access control lists on specialized CND systems (e.g., firewalls and intrusion prevention systems).

Perform system administration on specialized CND applications and systems (e.g., anti-virus, or Audit/Remediation) to include installation, configuration, maintenance, and backup/restore.

Implement C&A requirements for specialized CND systems within the NE or enclave, and document and maintain records for them.

Coordinate with the CND-A to manage and administer the updating of rules and signatures (e.g., IDS/IPS, anti-virus, and content blacklists) for specialized CND applications.

Administer CND test bed and test and evaluate new CND applications, rules/signatures, access controls, and configurations of CND-SP managed platforms.

Other

Collect and analyze intrusion artifacts (e.g., source code, malware, and trojans) and use discovered data to enable mitigation potential CND incidents within the enclave.

Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enclave systems.

Perform CND incident triage to include determining scope, urgency, and potential impact, identify the specific vulnerability and make recommendations which enable expeditious remediation.

Perform CND vulnerability assessments within the enclave.

Perform CND risk assessments within the enclave.

Conduct authorized penetration testing of enclave network assets.

Implement and enforce CND policies and procedures reflecting applicable laws, policies, procedures, and regulations

Provide incident reports, summaries, and other situational awareness information to higher headquarters..

Manage an incident (e.g., coordinate documentation, work efforts, resource utilization within the organization) from inception to final remediation and after action reporting.

Manage threat or target analysis of CND information and production of threat or target information within the network or enclave environment.

Manage the monitoring of external CND data sources to maintain enclave situational awareness.

Lead risk analysis and management activities for the network or enclave environment.

Track compliance audit findings, incident after-action reports, and recommendations to ensure appropriate mitigation actions are taken.

Analyze patterns of non-compliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats.

Other

ADDITIONAL DETAILS FOR FUNCTIONS