You will find the list below in Section B4 of the application where you will be able to identify the 5 tasks you are most familiar with. This sheet is for informational purposes only.

B4. **From the 74 Technical Level Tasks listed below, please identify a total of five (5) that you have performed and are the most familiar with. The five (5) tasks may be spread out across the technical levels.**

	Junior Technical Level Tasks
	Recognized a potential security violation, took appropriate action to report the incident as required by regulation, and mitigated any adverse impact.
	Applied instructions and pre-established guidelines to performed IA tasks within CE.
	Provided end user IA supported for all CE operating systems, peripherals, and applications.
	Supported, monitor, test, and troubleshoot hardware and software IA problems pertaining to their CE.
	Applied CE specific IA program requirements to identified areas of weakness.
	Applied appropriate CE access controls.
	Installed and operated the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards.
	Conduct tests of IA safeguards in accordance with established test plans and procedures.
	Implemented and monitor IA safeguards for CE system(s) in accordance with Implementation plans and standard operating procedures.
	Applied established IA security procedures and safeguards and comply with responsibilities of assignment.
	Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.
	Implemented online warnings to inform users of access rules for CE systems.
	Implemented applicable patches including IA vulnerability alerts (IAVA), IA vulnerability bulletins (IAVB), and technical advisories (TA) for the CE operating system(s).
	Installed, test, maintain, and upgrade CE operating systems software and hardware to comply with IA requirements.
	Understand and Implemented technical vulnerability corrections.
	Entered assets in a vulnerability management system.
	Applied system security laws and regulations relevant to the CE being supported.
	Implemented DoD and DoD Component password policy.
	Implemented specific IA security countermeasures.
	Intermediate Technical Level Tasks
	Demonstrate expertise in IAT Level I CE knowledge and skills.
	Examine potential security violations to determine if the NE policy has been breached, assess the impact, and preserve evidence.

	Supported, monitor, test, and troubleshoot hardware and software IA problems pertaining to the NE.
	Recommend and schedule IA related repairs in the NE.
	Performed IA related customer supported functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the NE.
	Provided end user supported for all IA related applications for the NE.
	Analyzed patterns of non-compliance and took appropriate administrative or programmatic actions to minimize security risks and insider threats.
	Managed accounts, network rights, and access to NE systems and equipment.
	Analyzed system performance for potential security problems.
	Assess the performance of IA security controls within the NE.
	Identified IA vulnerabilities resulting from a departure from the Implementation plan or that were not apparent during testing.
	Provided leadership and direction to IA operations personnel.
	Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements.
	Installed, test, maintain, and upgrade network operating systems software and hardware to comply with IA requirements.
	Evaluated potential IA security risks and took appropriate corrective and recovery action.
	Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements.
	Diagnose and resolve IA problems in response to reported incidents.
	Research, evaluated, and Provided feedback on problematic IA trends and patterns in customer supported requirements.
	Ensure IAT Level I personnel are properly trained and have met OJT program requirements.
	Performed system audits to assess security related factors within the NE.
	Develop and Implemented access control lists on routers, firewalls, and other network devices.
	Installed perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic.
	Work with other privileged users to jointly solve IA problems.
	Write and maintain scripts for the NE.
	Demonstrate proficiency in applying security requirements to an operating system for the NE or CE used in their current position.
	Implemented applicable patches including IAVAs, IAVBs, and TAs for their NE.
	Adhere to IS security laws and regulations to supported functional operations for the NE.
	Implemented response actions in reaction to security incidents.
	Supported the design and execution of exercise scenarios.

	Supported Security Test and Evaluations (Part of C&A Process).
	Obtain and maintain IA certification appropriate to position.
	Senior Technical Level Tasks
	Mastery of IAT Level I and IAT Level II CE/NE knowledge and skills.
	Recommend, schedule, and/or Implemented IA related repairs within the enclave environment.
	Coordinate and/or Provided supported for all enclave applications and operations.
	Lead teams and/or supported actions to quickly resolve or mitigated IA problems for the enclave environment.
	Formulate or Provided input to the enclave's IA/IT budget.
	Supported the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements for the enclave.
	Identified and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
	Direct and/or Implemented operational structures and processes to ensure an effective enclave IA security program including boundary defense, incident detection and response, and key management.
	Provided direction and/or supported to system developers regarding correction of security problems identified during testing.
	Evaluated functional operation and performance in light of test results and make recommendations regarding C&A.
	Examine enclave vulnerabilities and determine actions to mitigated them.
	Monitor and evaluated the effectiveness of enclave IA security procedures and safeguards.
	Analyzed IA security incidents and patterns to determine remedial actions to correct vulnerabilities.
	Supported development and/or Implementation of the enclave termination plan to ensure that IA security incidents are avoided during shutdown and long term protection of archived resources is achieved.
	Implemented vulnerability countermeasures for the enclave.
	Provided supported for IA customer service performance requirements.
	Provided supported for the development of IA related customer supported policies, procedures, and standards.
	Write and maintain scripts required to ensure security of the enclave environment.
	Implemented and maintain perimeter defense systems including, but not limited to, intrusion detection systems, firewalls, grid sensors.
	Schedule and performed regular and special backups on all enclave systems.
	Establish enclave logging procedures to include: important enclave events; services and proxies; log archiving facility.
	Provided OJT for IAT Level I and II DoD personnel.
	Analyzed IAVAs and Information Assurance Vulnerability Bulletins for enclave impact and took or recommend appropriate action.
	Obtain and maintain IA certification appropriate to position.

B7 Choose a total of three (3) Technical Level Tasks from the five (5) you identified and:

a. explain in narrative form what your specific role was in that task.
b. provide an evidentiary explanation of the implementation of the task.
c. describe the impact to the organization as a result of your expertise/effort.

***** ***Your Technical Level Task narrative should be no more than 500 words per task and should be double spaced. No handwritten narratives will be accepted.***