

Table C3.T7. IAT Level III Functions

T-III.1.	Mastery of IAT Level I and IAT Level II CE/NE knowledge and skills.
T-III.2.	Recommend, schedule, and/or implement IA related repairs within the enclave environment.
T-III.3.	Coordinate and/or provide support for all enclave applications and operations.
T-III.4.	Lead teams and/or support actions to quickly resolve or mitigate IA problems for the enclave environment.
T-III.5.	Formulate or provide input to the enclave's IA/IT budget.
T-III.6.	Support the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements for the enclave.
T-III.7.	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
T-III.8.	Direct and/or implement operational structures and processes to ensure an effective enclave IA security program including boundary defense, incident detection and response, and key management.
T-III.9.	Provide direction and/or support to system developers regarding correction of security problems identified during testing.
T-III.10.	Evaluate functional operation and performance in light of test results and make recommendations regarding C&A.
T-III.11.	Examine enclave vulnerabilities and determine actions to mitigate them.
T-III.12.	Monitor and evaluate the effectiveness of enclave IA security procedures and safeguards.
T-III.13.	Analyze IA security incidents and patterns to determine remedial actions to correct vulnerabilities.
T-III.14.	Support 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.
T-III.15.	Implement vulnerability countermeasures for the enclave.
T-III.16.	Provide support for IA customer service performance requirements.
T-III.17.	Provide support for the development of IA related customer support policies, procedures, and standards.
T-III.18.	Write and maintain scripts required to ensure security of the enclave environment.
T-III.19.	Implement and maintain perimeter defense systems including, but not limited to, intrusion detection systems, firewalls, grid sensors.
T-III.20.	Schedule and perform regular and special backups on all enclave systems.
T-III.21.	Establish enclave logging procedures to include: important enclave events; services and proxies; log archiving facility.
T-III.22.	Provide OJT for IAT Level I and II DoD personnel.
T-III.23.	Analyze IAVAs and Information Assurance Vulnerability Bulletins for enclave impact and take or recommend appropriate action.
T-III.24.	Obtain and maintain IA certification appropriate to position.