

Summary Report for Individual Task
805B-79T-4705
Mange Information Security (INFOSEC) for the ARNG Recruiting and Retention Command
Status: Approved

Distribution Restriction: Approved for public release; distribution is unlimited.

Destruction Notice: None

Foreign Disclosure: FD1 - The materials contained in this course have been reviewed by the course developers in coordination with the RRS, Fort Jackson foreign disclosure authority. This course is releasable to students from all requesting foreign countries without restrictions.

Condition: Given an office environment with the responsibility as the Information Assurance Security Officer (IASO) for the Recruiting and Retention Command and access to: AR 380-19 (Information Systems Security), Guidance from HRC-IAM, Guidance from NGB-ASM, State, and local SOP.

Standard MOPP 4 conditions do not exist for this task. See the MOPP 4 statement for specific conditions.

Standard: Manage INFOSEC for the Recruiting and Retention Command IAW AR 25-2, guidance from HRC-DAA, guidance from NGB-ASM, state and local guidance.

Special Condition: None

Safety Risk: Low

MOPP 4: N/A

Task Statements

Cue: None

DANGER
None

WARNING
None

CAUTION
None

Remarks: None

Notes: None

Performance Steps

1. Process and maintain appropriate security forms and paperwork.
 - a. Assignment of Information Support Specialist (IT II) as an Information Assurance Security Manager (IASM).
 - (1) Complete and submit USAAC Form 101. Refer to Automation System Support User Guide (ASSUG).
 - (2) Complete Additional Duty Appointment Memorandum from Command, refer to ASSUG.
 - (3) USAAC Non-Disclosure Agreement from Command, refer to ASSUG.
 - (4) USAAC Privileged-Level Access Agreement (PAA), refer to ASSUG.
 - (5) Complete DD Form 2842 to apply for ASCL CAC, refer to ASSUG.
 - b. Establish functional Users (IT III Users).
 - (1) Complete and submit USAAC Form 101. Refer to Automation System Support User Guide (ASSUG).
 - (2) Complete USAAC Acceptable Use Policy (AUP), refer to ASSUG.
 - (3) Complete memorandum for temporary access, if no security clearance granted, refer to Quick Reference – Unclassified IT Waivers Guide and appropriate waiver templates.
 - (4) Complete state AUP and other forms (as required), refer to ASSUG.
 - c. Maintain functional Users.
 - (1) Favorable adjudication of investigation, no further action required.
 - (2) Un-favorable adjudication of investigation.
 - (a) Refer to AR 25-2, Personnel Security Standards.
 - (b) Refer to Quick Reference – Unclassified IT Waivers Guide.
 - (c) Refer to appropriate waiver templates.
2. Conduct initial and annual physical security briefings IAW Army Road Warrior Laptop Security BBP and ASSUG.
3. Comply with DOD, NGB, USAREC, and State password conventions and policies.
4. Respond to INFOSEC violations IAW AR 25-1, AR 25-2, and AR 380-19. Some examples are:
 - a. Malware Alert.
 - b. Improper Use (AUP Violation).
 - c. Compromised System.
 - d. Loss of AIS.

(Asterisks indicates a leader performance step.)

Evaluation Guidance: Score "GO" if Soldier correctly performs all performance measures. Score "NO GO" if Soldier incorrectly performs one or more performance measure. Provide on-the-spot correction should the Soldier experience minor difficulty. Consider directing self-study or on-the-job-training for Soldiers who experience major difficulties in task performance.

Evaluation Preparation: This task may be evaluated by two methods;

a. Self Evaluation. Perform the task on the job using the materials listed in the Conditions Statement. Evaluate yourself, using the performance measures, graded IAW the Evaluation Guidance section.

b. Supervisor's Evaluation. Ensure that the soldier(s) have the material shown in the Condition Statement to accomplish the task. When you feel they are able, have them perform the task on the job. Grade them using the Performance Measures, IAW the Evaluation Guidance section.

PERFORMANCE MEASURES	GO	NO-GO	N/A
1. Processed and maintained appropriate security forms and paperwork.			
a. Assignment of Information Support Specialist (IT II) as an Information Assurance Technical Level 1 (IAT1).			
(1) Completed and submitted USAAC Form 101. Referred to Automation System Support User Guide (ASSUG).			
(2) Completed and submitted Additional Duty Appointment Memorandum from Command, referred to ASSUG.			
(3) Completed and submitted USAAC Non-Disclosure Agreement from Command, referred to ASSUG.			
(4) Completed and submitted USAAC Privileged-Level Access Agreement (PAA), referred to ASSUG.			
(5) Completed and submitted DD Form 2842 for ASCL CAC, referred to ASSUG.			
b. Established functional Users (IT III Users).			
(1) Completed and submitted USAAC Form 101. Referred to Automation System Support User Guide (ASSUG).			
(2) Completed USAAC Acceptable Use Policy (AUP), referred to ASSUG.			
(3) Completed memorandum for temporary access, if no security clearance granted, referred to Quick Reference – Unclassified IT Waivers Guide and appropriate waiver templates.			
(4) Completed state AUP and other forms (as required), referred to ASSUG.			
c. Completed state AUP and other forms (as required), referred to ASSUG.			
(1) Favorable adjudication of investigation, no further action required.			
(2) Un-favorable adjudication of investigation.			
(a) Referred to AR 25-2, Personnel Security Standards.			
(b) Referred to Quick Reference – Unclassified IT Waivers Guide.			
(c) Refer to appropriate waiver templates.			
2. Conduced initial and annual physical security briefings IAW Army Road Warrior Laptop Security BBP and ASSUG.			
3. Complied with DOD, NGB, USAREC, and State password conventions and policies.			
4. Responded to INFOSEC violations IAW AR 25-1, AR 25-2, and AR 380-19.			

Supporting Reference(s):

Step Number	Reference ID	Reference Name	Required	Primary
	AR 25-1	INFORMATION MANAGEMENT ARMY INFORMATION TECHNOLOGY	No	No
	AR 25-2	INFORMATION ASSURANCE (w/Chg 1, 23/03/2009)	No	No
	AR 380-19	Information System Security	No	No
	AR 380-5	DEPARTMENT OF THE ARMY INFORMATION SECURITY PROGRAM	No	No

Environment: Environmental protection is not just the law but the right thing to do. It is a continual process and starts with deliberate planning. Always be alert to ways to protect our environment during training and missions. In doing so, you will contribute to the sustainment of our training resources while protecting people and the environment from harmful effects. Refer to FM 3-34.5 Environmental Considerations and GTA 05-08-002 ENVIRONMENTAL-RELATED RISK ASSESSMENT.

Safety: In a training environment, leaders must perform a risk assessment in accordance with ATP 5-19, Risk Management. Leaders will complete the current Deliberate Risk Assessment Worksheet in accordance with the TRADOC Safety Officer during the planning and completion of each task and sub-task by assessing mission, enemy, terrain and weather, troops and support available-time available and civil considerations, (METT-TC). Note: During MOPP training, leaders must ensure personnel are monitored for potential heat injury. Local policies and procedures must be followed during times of increased heat category in order to avoid heat related injury. Consider the MOPP work/rest cycles and water replacement guidelines IAW FM 3-11.4, Multiservice Tactics, Techniques, and Procedures for Nuclear, Biological, and Chemical (NBC) Protection, FM 3-11.5, Multiservice Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Decontamination.

Prerequisite Individual Tasks : None

Supporting Individual Tasks : None

Supported Individual Tasks : None

Supported Collective Tasks : None

ICTL Data :

ICTL Title	Personnel Type	MOS Data
79T ARNG Recruiting and Retention-SL4	Enlisted	MOS: 79T, Skill Level: SL4, ASI: V7, Duty Pos: REA, SQI: 4