

Summary Report for Individual Task
805B-79T-4702
Maintain a Recruiter Work Station (RWS)
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 foreign disclosure authority. This course is releasable to students from all requesting foreign countries without restrictions.

Condition: Given an office environment, a malfunctioning and/or non-compliant RWS with access to appropriate software and/or replacement hardware, secondary administrative role for the RWS, Automation System Support User Guide, and necessary internet connectivity. Standard MOPP 4 conditions do not exist for this task. See the MOPP 4 statement for specific conditions.

Standard: Restore functionality and/or compliance with current RWS hardware and software baseline requirements.

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. Identify RWS maintenance required.
 - a. If the problem is hardware, go to Step 2.
 - b. If the problem is software, go to Step 5.
 - c. If the problem is network, go to Step 10.
2. Determine if hardware is under warranty by calling manufacturer or referencing manufacturer website.
 - a. If item is under warranty:
 - (1) Order a replacement.
 - (2) Receive order. (Go to Step 4)
 - b. If item is NOT under warranty, go to Step 3.
3. Determine if it is cost and/or time effective to repair equipment.
 - a. If yes, go to Step 4.
 - b. If no,
 - (1) Turn equipment into supply or destroy IAW local SOP.
 - (2) Order replacement equipment. (Go to Step 4)
4. Perform equipment repair/replacement, IAW applicable regulations and manuals.
 - a. If repaired, verify the problem is fixed.
 - (1) If yes, reissue equipment to end user.
 - (2) If no, go to Step 1.
 - b. If replaced, verify operability of the equipment.
 - (1) If yes, issue equipment to end user.
 - (2) If no, go to Step 1.
5. Determine if update / software, application, or driver issue.
 - a. Update / Software issue (Master Vulnerability Report (MVR), Security Inventory Report (SIR), McAfee (ePo), Information Assurance Vulnerability Alert (IAVA), Information Assurance Vulnerability Bulletin (IAVB), Information Assurance Vulnerability Technical (IAVT), Unmanaged Report (UMR), Support Bridge, Information Technology Client Manager (ITCM), Windows Server Update Services (WSUS), and other knowledge zone documents as applicable), go to Step 6.
 - b. If application issue, go to Step 7.

- c. If driver issue, go to Step 10.
- 6. Perform update using appropriate media or website.
 - a. If update is successful, end Task.
 - b. If update fails:
 - (1) Reference Knowledge Zone for fix.
 - (a) If fix available, end Task.
 - (b) If fix is unavailable, re-image equipment.
 - (2) Support Bridge.
 - (a) If fix available, end Task.
 - (b) If fix is unavailable, re-image equipment.
 - (3) Open CSC Help Desk Ticket.
- 7. Determine if software is baseline.
 - a. If yes, go to Step 8.
 - b. If no, remove software.
- 8. Determine if software is configured properly, IAW ABS Imaging Guide.
 - a. If yes, go to Step 9.
 - b. If no, configure software.
- 9. Research application error to see if a fix is available using knowledge zone documents.
 - a. Reference Knowledge Zone to fix.
 - (1) If fix available, end Task.
 - (2) If fix is unavailable, re-image equipment.
 - b. Access support bridge website for fix/patch.
 - (1) If fix available, end Task.
 - (2) If fix is unavailable, re-image equipment.
 - c. Search proprietary web site for software.

(1) If fix is available, end Task.

(2) If fix is unavailable, re-image equipment.

d. Repair/Reinstall Software.

(1) If fixed, end Task.

(2) If unable to fix, re-image equipment.

e. Open Headquarters Recruiting Command (HRC) Service Desk Ticket.

10. Determine if current driver is properly installed IAW ABS Imaging Guide.

a. If yes, go to Step 11.

b. If no, install the correct driver.

(1) Reboot.

(2) Verify functionality.

11. Configure the device.

a. Verify functionality.

b. Redo steps 10 and 11. NOTE: Do not do this more than twice.

12. Re-image the RWS IAW Current ABS Imaging Guide.

NOTE: Most common network/connectivity issues can be identified by checking the following areas:

a. Devices working.

b. Cabling/wireless point/aircard.

c. Outgoing pipe issues/ie settings.

d. VPN issues.

e. Problem on the other end.

(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. Identified RWS maintenance as required.			
a. If the problem was hardware, went to Step 2.			
b. If the problem was software, went to Step 5.			
c. If the problem was network, went to Step 10.			
2. Determined if hardware was under warranty, called manufacturer or referenced manufacturer website.			
a. If item was under warranty:			
(1) Ordered a replacement.			
(2) Received order. (Went to Step 4)			
b. If item was NOT under warranty, went to Step 3.			
3. Determined if it was cost and/or time effective to repair equipment.			
a. If yes, went to Step 4.			
b. If no,			
(1) Turned equipment into supply or destroyed IAW local SOP.			
(2) Ordered replacement equipment, went to Step 4).			
4. Performed equipment repair/replacement, IAW applicable regulations and manuals.			
a. If repaired, verified the problem was fixed.			
(1) If yes, reissued equipment to end user.			
(2) If no, went to Step 1.			
b. If replaced, verified operability of the equipment.			
(1) If yes, issued equipment to end user.			
(2) If no, went to Step 1.			
5. Determined if update / software, application, or driver issue.			
a. Updated / Software issued (Master Vulnerability Report (MVR), Security Inventory Report (SIR), McAfee (ePo), Information Assurance Vulnerability Alert (IAVA), Information Assurance Vulnerability Bulletin (IAVB), Information Assurance Vulnerability Technical (IAVT), Unmanaged Report (UMR), Support Bridge, Information Technology Client Manager (ITCM), Windows Server Update Services (WSUS), and other knowledge zone documents as applicable), went to Step 6.			
b. If application issued, went to Step 7.			
c. If driver issued, went to Step 10.			
6. Performed update using appropriate media or website.			
a. If update was successful, ended Task.			
b. If update failed:			
(1) Referenced Knowledge Zone for fix.			
(a) If fix was available, ended Task.			
(b) If fix was unavailable, re-imaged equipment.			
(2) Support Bridge.			
(a) If fix was available, ended Task.			
(b) If fix was unavailable, re-imaged equipment.			
(3) Opened HRC Service Desk Ticket.			
7. Determined if software was baseline.			
a. If yes, went to Step 8.			
b. If no, removed software.			
8. Determined if software was configured properly, IAW ABS Imaging Guide.			
a. If yes, went to Step 9.			
b. If no, configured software.			
9. Researched application error to see if a fix was available using knowledge zone documents.			
a. Referenced Knowledge Zone to fix.			
(1) If fix was available, ended Task.			

(2) If fix was unavailable, re-imaged equipment.			
b. Accessed support bridge website for fix/patch.			
(1) If fix was available, ended Task.			
(2) If fix was unavailable, re-imaged equipment.			
c. Searched proprietary web site for software.			
(1) If fix was available, ended Task.			
(2) If fix was unavailable, re-imaged equipment.			
d. Repaired/Reinstalled Software.			
(1) If fixed, ended Task.			
(2) If unable to fix, re-imaged equipment.			
e. Opened Headquarters Recruiting Command (HRC) Service Desk Ticket.			
10. Determined if current driver was properly installed, IAW ABS.			
a. If yes, went to Step 11.			
b. If no, installed the correct driver.			
(1) Rebooted.			
(2) Verified functionality.			
11. Configured the device.			
a. Verified functionality.			
b. Redid steps 10 and 11.			
12. Re-imaged the RWS IAW Current ABS Imaging Guide.			

Supporting Reference(s): None

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