PUBLICATION

EXAM-TM40E-PRE

PRE-TEST — SL 4E: PROTECTION

Maven Smart System (MSS) — USAREUR-AF

HEADQUARTERS
UNITED STATES ARMY EUROPE AND AFRICA
(USAREUR-AF)
Wiesbaden, Germany

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

PRE-TEST — SL 4E: PROTECTION

MAVEN SMART SYSTEM (MSS) — USAREUR-AF

Field	Detail
Course	SL 4E: Protection WFF Track
Form	Pre-Test
Level	SL 4E (WFF Track)
Audience	Force protection officers, CBRN officers, provost marshal staff, G2/S2 force protection analysts; prerequisite: SL 1 + SL 2 + SL 3 complete
Time Allowed	20 minutes
Passing Score	N/A — diagnostic only

INSTRUCTIONS

This diagnostic assessment establishes your baseline knowledge before training. Your score does not affect course eligibility. Answer honestly — results help the instructor tailor instruction to identified gaps.

SECTION 1 — MULTIPLE CHOICE

Circle the letter of the best answer. (2 points each)

1. When displaying IED reporting data on the MSS COP, the protection officer's most important data quality check before a protection working group is:

A. Verify the data-as-of timestamp for the threat reporting feed — IED data that is 24–48 hours old may not reflect current threat conditions on routes or in the AOR B. Verify the symbology matches FM 1-02.1 standards C. Confirm that all reports have been validated by theater intelligence D. Ensure IED reports

are displayed using red symbols only

2. Threat trending analysis in MSS is best used to:

A. Predict the exact time and location of the next threat event B. Identify patterns in threat data over time — location clusters, event type trends, and time-of-day patterns — to support protection planning decisions C. Replace the intelligence preparation of the battlefield (IPB) process D. Generate automated force protection orders

3. A vulnerability assessment is being conducted using MSS data. Which statement best describes the limitation of this data?

A. MSS vulnerability data is classified and cannot be accessed by force protection officers B. Vulnerability assessment data in MSS is real-time and eliminates the need for physical site surveys C. MSS can display reported threat data and unit locations; vulnerability assessment requires human judgment to evaluate those factors against protection capabilities and gaps — MSS does not generate vulnerability scores D. MSS vulnerability overlays are binding — assessed vulnerabilities must be reported to theater immediately

4. CBRN sensor data can be integrated into MSS to support protection operations. The key limitation a CBRN officer must understand is:

A. CBRN data requires a separate platform and cannot be displayed alongside maneuver data B. Once a CBRN hazard area is displayed in MSS, it cannot be modified until theater approves C. CBRN data in MSS is automatically updated by the theater chemical officer D. CBRN sensor data feeds may have latency, coverage gaps, and sensor reliability variability — displayed hazard boundaries should be treated as estimated, not definitive

5. A force protection CCIR configured in MSS to alert when threat reporting in a defined area exceeds a threshold fires unexpectedly. The protection officer should:

A. Verify the alert by checking the data source, reviewing the raw reports, and assessing whether the reports reflect a genuine threat pattern or are duplicates or reporting artifacts before escalating B. Immediately execute the force protection plan without investigation C. Dismiss the alert and reconfigure the threshold higher to reduce false positives D. Transfer the alert to the S2 — force protection CCIRs are an intelligence function

6. Personnel accountability data (PERSTAT) in MSS provides:

A. Real-time GPS location tracking for every Soldier in the AOR B. Reported personnel strength by unit as of the last PERSTAT submission — not real-time individual tracking C. Automated accountability reports that replace the unit's morning formation requirement D. Classified personnel records that are not accessible below battalion level

7. Area security data displayed on the MSS COP is most useful for the protection working group when it:

A. Shows all terrain features in the AOR with no filter applied B. Includes only incidents that have been confirmed by military police reporting channels C. Is limited to the past 24 hours of data to prevent information overload D. Displays threat reporting, patrol sectors, checkpoint locations, and friendly unit positions together — enabling the working group to assess security coverage and identify gaps

8. Which of the following describes a correct OPSEC consideration for protection data products in MSS?

A. Force protection data is administrative and does not require distribution controls B. OPSEC applies only to intelligence data, not force protection data C. Threat reporting locations, patrol patterns, checkpoint positions, and PERSTAT data — in combination — reveal security posture and potential gaps; this aggregate must be protected and distributed only to those with operational need to know D. PERSTAT data is unclassified and can be shared freely within the brigade

SECTION 2 — SHORT ANSWER

Answer in 2–4 sentences. (5 points each)

9. You are a force protection officer preparing for the weekly protection working group. The MSS threat display shows three IED incidents in the past seven days along Route BROWN. What additional information do you need from the MSS data before presenting this information to the protection working group, and what would you caution the group about when interpreting the display?

(Write your answer below)

10. Describe the difference between what a PERSTAT in MSS tells you and what it does not tell you. Give one example of a decision a provost marshal should not make based solely on PERSTAT data in MSS.

(Write your answer below)

SECTION 3 — SCENARIO (10 POINTS)

Read the following scenario and answer the question.

Your BCT is beginning a new rotation. The protection officer has directed you to configure the MSS COP to support the protection working group. Requirements: display threat reporting for the past 30 days, configure a CCIR that alerts when threat reporting in Sector NORTH exceeds three events per week, and display PERSTAT for all organic battalions.

11. Describe how you would approach configuring these three elements in MSS. For each element, describe what data source you would select, what you would verify before the working group, and what limitation you would communicate to the protection officer about each display.

(Write your answer below)

Total points: 30. Diagnostic only — score does not affect course admission.

USAREUR-AF Operational Data Team EX_TM40E-PRE | Version 1.0 | March 2026

ANSWER KEY — INSTRUCTOR USE ONLY

Do not distribute to students. Use to identify baseline gaps and tailor Day 1 instruction accordingly.

Multiple Choice:

1. A — Verify the data-as-of timestamp for the threat reporting feed; IED data 24–48 hours old may not reflect current threat conditions. Symbology and theater validation are secondary checks.
2. B — Threat trending analysis identifies patterns in threat data over time to support protection planning; it does not predict specific events or replace IPB.
3. C — MSS displays reported threat data and unit locations; vulnerability assessment requires human judgment against protection capabilities and gaps — MSS does not generate vulnerability scores.
4. D — CBRN sensor data has latency, coverage gaps, and sensor reliability variability; displayed hazard boundaries should be treated as estimated, not definitive.

5. A — Verify the alert by checking the data source, reviewing raw reports, and assessing whether the reports reflect a genuine pattern or are duplicates/artifacts before escalating; do not immediately execute, dismiss, or transfer.
6. B — PERSTAT provides reported personnel strength from the last submission — not real-time individual GPS tracking or accountability at the individual level.
7. D — Area security data is most useful when it displays threat reporting, patrol sectors, checkpoint locations, and friendly positions together to enable gap assessment.
8. C — Threat locations, patrol patterns, checkpoints, and PERSTAT data in combination reveal security posture and gaps; the aggregate must be protected and distributed only to those with operational need to know.

Short Answer Guidance:

SA-9. Full credit (5 pts): Check the data-as-of timestamp for the IED reporting feed to confirm the three incidents fall within a current reporting window; determine whether the three incidents are in the same exact grid (possible duplicate reporting vs. three distinct events); during the working group, characterize the cluster as "three reported incidents on Route BROWN as of [data currency timestamp]" and caution the group that absence of additional reporting does not confirm the route is clear — it may indicate a reporting gap. Partial credit (3 pts): addresses data currency or the duplicate-reporting question but not both; or fails to address the caution about interpreting absence of reporting.

SA-10. Full credit (5 pts): PERSTAT shows reported personnel strength at the time of the last submission — it does not show individual Soldier locations, individual accountability, or changes since submission; a provost marshal should not make individual accountability decisions (e.g., declaring a Soldier AWOL or missing) based solely on a PERSTAT aggregate in MSS — individual accountability requires direct verification with the Soldier's chain of command. Any reasonable example of an individual-level decision is acceptable. Partial credit (3 pts): correctly describes the limitation without a concrete example of a decision that should not be made.

Scenario Guidance:

Q-11. Full credit (10 pts): Must address all three elements with data source, verification, and limitation for each.

Threat reporting (30 days): data source = threat reporting dataset with a 30-day time filter; verify the data-as-of timestamp and confirm the reporting feed is current; limitation = shows reported incidents only, not incidents that were not reported or not confirmed — coverage gaps in the reporting chain will appear as absence of incidents.

CCIR — Sector NORTH events > 3/week: data source = threat reporting dataset; configure geographic trigger with Sector NORTH boundary polygon; threshold = count of threat events within polygon exceeds 3 in a 7-day rolling window; route to FP officer and CDR; limitation = count accuracy depends entirely on all incidents being reported into the MSS feed — underreporting will produce false negatives.

PERSTAT display: data source = personnel reporting dataset linked to PERSTAT submissions from organic battalions; verify all three battalions have submitted within the current PERSTAT cycle before the working group; limitation = reflects last submission only; does not capture changes (casualties, gains) since the last submission.

Partial credit (6 pts): two of three elements addressed correctly with all three required sub-elements (source, verification, limitation). Minimum acceptable: two elements with at least data source and limitation described.

USAREUR-AF Operational Data Team EX_TM40E-PRE | Answer Key | Version 1.0 | March 2026