PUBLICATION

EXAM-TM40E-POST

POST-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

POST-TEST — SL 4E: PROTECTION

MAVEN SMART SYSTEM (MSS) — USAREUR-AF

Field	Detail
Course	SL 4E: Protection WFF Track
Form	Post-Test
Level	SL 4E (WFF Track)
Audience	Force protection officers, CBRN officers, provost marshal staff; prerequisite: completion of SL 4E training
Time Allowed	30 minutes
Passing Score	80% (32/40 points)

INSTRUCTIONS

This assessment confirms proficiency upon completion of SL 4E training. A score of 80% (32/40) is required for course completion certification. Results are recorded on the student training record.

SECTION 1 — MULTIPLE CHOICE

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

1. You have configured a force protection CCIR in MSS to alert when a threat event occurs within the restricted area boundary surrounding FOB KESTREL. During the protection working group, a threat event is reported inside the boundary but the CCIR does not fire. The most likely cause is:

A. The geographic boundary in the CCIR definition does not correctly match the restricted area — the boundary was entered with incorrect coordinates or default dimensions B. CCIR geographic alerts require 30-minute polling intervals — the event has not yet been processed C. CCIR alerts only function when

the MSS operator is actively logged in D. Threat events must be confirmed by the S2 before a CCIR can trigger

2. The Sector SOUTH threat reporting feed stops updating 90 minutes before the protection working group. Before briefing the commander, you should:

A. Extrapolate threat activity in Sector SOUTH based on the most recent data trend and brief it as current B. Mark Sector SOUTH data as stale on all displayed products, caveat any Sector SOUTH information as "last reported [time]," and contact the Sector SOUTH reporting element for a spot report C. Remove Sector SOUTH from the threat display to avoid confusion until the feed is restored D. Delay the protection working group until the Sector SOUTH feed is restored

3. PERSTAT displayed in MSS shows 3rd Battalion at 91% personnel present for duty. Before briefing this figure to the protection working group, you must:

A. Confirm the figure with 3rd Battalion S1 — PERSTAT in MSS is never authoritative B. Convert the percentage to a headcount before briefing — percentages are not acceptable in a protection product C. Verify the data-as-of timestamp — PERSTAT in MSS reflects the last submitted report, not real-time accountability D. Obtain the battalion commander's approval to brief 3rd Battalion personnel data to the working group

4. A CBRN officer is integrating synthetic hazard sensor data into the MSS COP. The officer displays a hazard boundary and briefs the protection working group that the affected area is confirmed. The correct characterization of this information is:

A. Confirmed — sensor data in MSS reflects validated CBRN readings B. Classified — CBRN hazard boundaries cannot be briefed below theater level C. Preliminary — all CBRN data requires 24-hour laboratory confirmation before display in MSS D. Estimated — CBRN sensor feeds may have latency, coverage gaps, and sensor reliability variability; the displayed boundary is a model estimate, not a confirmed boundary

5. Your force protection CCIR for casualties above threshold fires unexpectedly during a routine training period when no casualties have been reported. The correct first action is:

A. Verify the alert by checking the casualty data source, reviewing the raw records that triggered the threshold, and confirming whether the trigger reflects a genuine event or a data entry error before escalating B. Execute force protection Plan B immediately — the CCIR system does not produce false positives C. Reconfigure the casualty threshold to a higher value to eliminate false positives D. Transfer CCIR monitoring to the S1 — casualty data is a personnel function

6. A vulnerability assessment display in MSS shows three IED events along MSR BRONZE in the past 14 days. When briefing this to the protection working group, the force protection officer should:

A. Declare MSR BRONZE a restricted route and initiate route closure procedures B. Present the data pattern as a potential indicator requiring further assessment — note the data source, the time window, and the fact that MSS displays reported incidents, not a confirmed threat assessment C. Remove the

events from the display unless confirmed by theater intelligence D. Brief the route as safe — three events in 14 days is below the theater reporting threshold

7. For OPSEC purposes, force protection products containing threat locations, PERSTAT data, and vulnerability overlays should be:

A. Shared broadly within the brigade to maximize situational awareness B. Exported to PDF and emailed to all working group attendees after each meeting C. Classified at the SECRET level automatically when threat data is included D. Treated as sensitive in aggregate — individually some elements may be unclassified, but the combination reveals security posture and gaps and must be distributed only to those with operational need to know

8. When a threat reporting feed fails during a protection working group, the force protection officer's primary responsibility is:

A. Fix the pipeline immediately — the working group cannot proceed without complete data B. Suspend the working group until full data coverage is restored C. Characterize the data gap clearly to the protection working group, identify what decisions are and are not supportable with current data, and assign follow-on action to restore or verify the feed D. Contact the software vendor to report the feed failure

9. ADP 3-37 establishes CVP (Criticality-Vulnerability-Probability) analysis as the framework for protection prioritization (section 4-2a). Which of the following correctly describes the three CVP factors?

A. Criticality = how exposed the asset is to threats; Vulnerability = how important the asset is to mission success; Probability = how quickly the asset can be replaced B. Criticality = how important the asset is to mission success; Vulnerability = how exposed the asset is to threats; Probability = how likely the threat is to act against this asset C. Criticality = how likely the threat is to act; Vulnerability = how quickly the asset can recover; Probability = how important the asset is to mission success D. Criticality = how hardened the asset is; Vulnerability = how many countermeasures are in place; Probability = the historical frequency of attacks in the AOR

10. The OPSEC 5-step process (FM 3-13.3) maps to data security practices on MSS (section 4-7, Table 4-2). What is the correct sequence of the five OPSEC steps?

A. Analyze threats, identify critical information, assess risk, analyze vulnerabilities, apply countermeasures B. Apply countermeasures, analyze threats, assess risk, identify critical information, analyze vulnerabilities C. Identify critical information, analyze threats, analyze vulnerabilities, assess risk, apply countermeasures D. Assess risk, identify critical information, analyze threats, apply countermeasures, analyze vulnerabilities

SECTION 2 — SHORT ANSWER

Answer in 3–5 sentences. (5 points each)

11. Your CCIR for threat events in the restricted area has not fired in the past 72 hours, but the S2 reports that a threat event occurred within the restricted area 24 hours ago. Walk through the troubleshooting steps you would take to determine why the CCIR did not fire and what corrective action you would take before the next protection working group.

(Write your answer below)

12. The provost marshal asks why the MSS PERSTAT display shows 1st Battalion at 94% PFD when the battalion S1 verbally confirmed 87% PFD this morning. Explain the possible reasons for this discrepancy and describe how you would characterize the PERSTAT data to the protection working group until the discrepancy is resolved.

(Write your answer below)

SECTION 3 — SCENARIO (10 POINTS)

Read the following scenario and answer the question below.

It is 1345. The protection working group begins at 1415. You open MSS and discover: - Threat reporting from Sector SOUTH has not updated since 1145 (2 hours old) - The CCIR for threat events in the restricted area has not fired in 72 hours, but the threat display shows two events near the boundary that may be within the restricted area - The PERSTAT display is current for all units (last submitted 1300) - The protection working group will include the BCT commander and the adjacent unit's force protection officer

You have 30 minutes before the working group.

13. Describe your complete course of action for the next 30 minutes. Include: (a) what you will investigate first and why, (b) what you will brief versus what you will caveat, (c) how you will characterize the Sector SOUTH data gap and the CCIR anomaly to the commander, and (d) what follow-on actions you will assign before the working group ends.

(Write your answer below)

ANSWER KEY (INSTRUCTOR USE ONLY — DO NOT DISTRIBUTE)

Section 1: 1. A — incorrect boundary coordinates are the most common geographic CCIR failure; the boundary must precisely match the restricted area specification 2. B — characterize the gap, caveat all affected products, request a spot report; do not extrapolate, remove, or delay 3. C — PERSTAT reflects the last submitted report; timestamp verification is mandatory before briefing 4. D — CBRN hazard boundaries from sensor feeds are estimates, not confirmed areas; this is a critical safety and operational distinction 5. A — verify before escalating; the CCIR system can produce false positives from data entry errors 6. B — present the data pattern with context; do not make route closure decisions unilaterally from MSS data alone 7. D — aggregate sensitivity applies; the combination of threat locations, PERSTAT, and vulnerability data reveals security posture 8. C — characterize, identify decision impact, assign follow-on; do not fix the pipeline at this level

Section 2 — Expected elements: 11. Should include: check the CCIR boundary definition against the restricted area coordinates; check whether the event that the S2 reported was entered in the correct data source feeding the CCIR; verify the event coordinates are actually within the boundary (boundary entry errors are common); test the CCIR with the known event location using the test dataset; if the CCIR boundary is confirmed wrong, update it and document the correction before the next working group. 12. Should explain: PERSTAT in MSS reflects the last submitted report, which may not be the same as the battalion's most recent accountability formation; pipeline latency between the S1's submission and the MSS dataset update could account for the gap; a submission may not have been entered through the channel that feeds MSS; characterize to the working group by presenting both figures with timestamps and noting the discrepancy is being researched — do not brief either figure as definitive until the source of the difference is identified.

Section 3 — Expected elements: (a) Investigate the CCIR boundary anomaly first — two events near the restricted area boundary that may not have triggered the CCIR is a potential operational gap that affects the commander's decision calculus immediately; the Sector SOUTH staleness is also critical but the CCIR issue is both a data quality problem and a potential threat indicator. (b) Brief: PERSTAT as current (data is timely and complete); threat trends for Sector NORTH and CENTRAL as current. Caveat: Sector SOUTH threat data as of 1145 (2 hours old — unknown current threat conditions in that sector); the two near-boundary events as "requiring confirmation of exact coordinates before CCIR applicability can be determined." (c) Tell the commander: Sector SOUTH threat reporting has a 2-hour gap — current threat conditions in that sector are unconfirmed; the working group should note this uncertainty for any decisions affecting Sector SOUTH routes or assets. On the CCIR: two events show on the display near the restricted area boundary; the CCIR did not fire, which may indicate a boundary configuration issue or that the events are outside the boundary — this is being investigated and you will have a definitive answer before the end of the working group. (d) Assign: S6 to investigate the Sector SOUTH feed and report restoration status; S2/patrol element to provide a spot report on Sector SOUTH current conditions; self-action to verify CCIR boundary coordinates against restricted area specification and test the two near-boundary events before the working group closes — report finding to the protection working group before adjournment.

Total points: 40 (MC: 10 × 2 = 20, SA: 2 × 5 = 10, Scenario: 10). Passing score: 32 (80%).

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