COURSE SYLLABUS

SL 4E

USAREUR-AF

COURSE SYLLABUS — SL 4E: PROTECTION WARFIGHTING FUNCTION

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

COURSE SYLLABUS — SL 4E: PROTECTION WARFIGHTING FUNCTION

MAVEN SMART SYSTEM (MSS) — USAREUR-AF

Field	Detail
Level	SL 4E — Protection WFF Track
Duration	3 days (24 hours)
Prerequisites	SL 1, SL 2, SL 3 (Go evaluations on file); CONCEPTS_GUIDE_TM40E_PROTECTION (required reading before Day 1)
Audience	Force protection officers, CBRN officers, provost marshal staff, and G2/S2 force protection analysts at BCT echelon and below
Format	Instructor-led seminar + demonstration + tabletop exercise + practical evaluation
Location	MSS Training Environment (standard user access sufficient)

BLUF: SL 4E teaches protection staff to integrate MSS into force protection workflows — tracking threat activity, visualizing installation and route vulnerability, managing force protection CCIR alerts, displaying CBRN sensor data, and maintaining PERSTAT accountability. Course applies MSS capabilities to processes in ADP 3-37 and ATP 3-37.2. No coding or pipeline experience required.

LEARNING OBJECTIVES

#	Objective
1	Configure threat data layers on the COP — threat incident reporting, IED reporting, threat trend overlays — with data freshness verification and source attribution
2	Build vulnerability assessment visualization: installation perimeter overlays, route vulnerability displays, and threat-to-friendly exposure analysis

#	Objective
3	Configure force protection CCIR alerts — threat-in-area triggers, casualty threshold notifications, and CBRN event alerts
4	Display CBRN sensor data and contamination overlays, including hazard area visualization and downwind hazard estimate displays
5	Build and maintain a PERSTAT display and accountability status dashboard integrating strength data with data-as-of timestamps
6	Identify and respond to threat reporting gaps or CBRN data staleness before a protection working group
7	Apply OPSEC procedures to force protection products: classification markings, distribution restrictions, handling instructions for friendly vulnerability information
8	Characterize threat reporting gaps accurately — covering known threats, assessed threats, and areas with insufficient current reporting — without overstating or understating risk

PRE-COURSE CHECKLIST

Complete **5+ duty days before Day 1:**

- ☐ Read CONCEPTS_GUIDE_TM40E_PROTECTION in full — Day 1 builds directly on it
- ☐ Confirm MSS training account is active
- ☐ Bring your unit's current force protection CCIR list or a threat reporting format from a recent exercise — used during the Day 1 CCIR configuration lab
- ☐ Review your installation or AOR's current CBRN reporting format — Day 2 asks you to replicate a CBRN data overlay in MSS

DAILY SCHEDULE

Day 1 — Threat Data Layers and Force Protection COP Configuration

Time	Block	Method	Content
0800–0900	1	Brief	Doctrinal context: ADP 3-37; how MSS supports force protection visibility; role of the protection COP in the operations process

Time	Block	Method	Content
0900–1100	2	Demo/Lab	Threat data layer configuration: threat incident layers, IED reporting feeds, and threat trend overlays; data sources, display standards, and source attribution
1100–1115	—	Break	
1115–1200	3	Lab	Vulnerability assessment visualization: installation perimeter overlays, route vulnerability displays, cross-referencing threat layers with friendly position data
1200–1300	—	Lunch	
1300–1500	4	Lab	Force protection CCIR configuration: translating commander's published CCIRs into MSS alert thresholds; geographic triggers, casualty thresholds, CBRN event alerts
1500–1515	—	Break	
1515–1700	5	Exercise	CCIR drill: given force protection CCIRs and a sample threat dataset, configure 3 force protection CCIRs and verify they trigger correctly

Evening reading: TM-40E, Chapter 4 (Antiterrorism and Force Protection) — source attribution requirements and difference between reported threat incidents and assessed threat patterns.

Day 2 — CBRN Data Visualization, PERSTAT, and Vulnerability Assessment

Time	Block	Method	Content
0800–0830	—	Review	Day 1 questions; CCIR configuration review — common threshold errors for geographic and event-type triggers
0830–1030	6	Demo/Lab	CBRN data display: CBRN sensor feed layers, contamination overlay displays, downwind hazard estimate visualization; data currency requirements for CBRN products
1030–1045	—	Break	
1045–1200	7	Lab	PERSTAT and accountability dashboard: building a PERSTAT display integrating strength reporting from subordinate elements; configuring accountability status indicators with data-as-of timestamps
1200–1300	—	Lunch	

Time	Block	Method	Content
1300–1500	8	Demo/Lab	Integrated protection picture: combining threat overlays, CBRN data, vulnerability assessments, and PERSTAT into a protection working group product for O-4/O-5 audience
1500–1515	—	Break	
1515–1700	9	Exercise	Protection product drill: build a CBRN overlay and PERSTAT display from a provided dataset; evaluator reviews for data currency, timestamp placement, and OPSEC marking

Evening reading: TM-40E, Chapter 3 (CBRN Defense Operations) and Chapter 2 (Composite Risk Management in MSS).

Day 3 — Threat Reporting Gaps, Degraded Procedures, and Practical Exercise

Time	Block	Method	Content
0800–0900	10	Brief	Threat reporting gaps: procedures when reporting from a sector stops updating; risk of over- or under-characterizing threat based on stale data; escalation path and caveat requirements
0900–1030	11	Demo/Lab	Degraded protection picture: maintaining force protection products with partial threat or CBRN data; manual backup procedures; what to brief to the commander when sensor data is unavailable
1030–1045	—	Break	
1045–1100	12	Brief	Practical exercise scenario brief; product standards checklist review; protection working group tabletop ground rules
1100–1200	—	Prep	Practical exercise setup and planning time
1200–1300	—	Lunch	
1300–1700	13	**Eval**	**Practical exercise:** configure force protection COP, build CBRN overlay and PERSTAT display, configure force protection CCIRs, respond to a threat reporting gap inject, brief findings to evaluator in role as S3

REQUIRED READING

When	Reading
Before Day 1	CONCEPTS_GUIDE_TM40E_PROTECTION (complete)
Day 1 evening	TM-40E, Ch 4 (Antiterrorism and Force Protection)
Day 2 evening	TM-40E, Ch 3 (CBRN Defense Operations)
Day 2 evening	TM-40E, Ch 2 (Composite Risk Management in MSS)
Day 3 (review)	TM-40E, Ch 10 (Degraded Operations) — skim before Day 3 brief

PRACTICAL EXERCISE

Scenario: You are the force protection section at a BCT headquarters during an exercise. The S3 requires a configured force protection COP — threat overlays, CBRN sensor display, PERSTAT dashboard, and force protection CCIRs active — before a protection working group in four hours. At T+90 minutes, threat reporting from one sector stops updating.

#	Task
1	Configure force protection COP layers — threat incident overlay, IED reporting feed, and vulnerability assessment display — and verify data currency for all feeds
2	Build a CBRN sensor and contamination overlay using the provided synthetic CBRN data, including a downwind hazard estimate display
3	Configure 3 force protection CCIRs from the provided commander's guidance card, including a threat-in-area trigger and a CBRN event alert
4	Build a PERSTAT accountability dashboard integrating strength data from all subordinate elements with data-as-of timestamps
5	Respond to the threat reporting sector staleness inject: identify affected COP areas, apply correct caveats, characterize the reporting gap to the evaluator, and brief what the commander can and cannot conclude about threat status in the affected sector
6	Apply OPSEC procedures to the final force protection working group product before simulated distribution

Go standard: Pass 5 of 6 tasks. No-Go on Task 3 (CCIR configuration) or Task 5 (data staleness response) = automatic No-Go regardless of total score.

GO CRITERIA

Task	Hard Standard
Force protection products	Every threat incident on the COP must have a source AND a timestamp — the evaluator will ask how you know the data is current and where it came from
PERSTAT dashboard	Data-as-of timestamps required at the **element level** — a single page-level timestamp without element-level currency indicators fails Task 4
Data staleness inject	Both overstating risk (treating sector as unmonitored when other indicators remain current) and understating risk (treating stale-reporting sector as fully covered) are No-Go. Evaluator probe: "What do you know, what are you estimating, and what are you telling the commander?"

Function-Specific Go Criteria — Protection

Criterion	Standard
CBRN contamination overlay	Contamination overlay must include a downwind hazard estimate layer — a contamination display without downwind projection fails the CBRN visualization element
PERSTAT accountability	PERSTAT dashboard must show unit accountability by company-level subordinate unit — battalion-level rollup only is insufficient for force protection purposes
Threat characterization	When responding to the threat reporting staleness inject, trainee must not overstate risk ("area is clear") or understate it ("sector is fully covered") — correct answer explicitly characterizes the gap and communicates uncertainty to the commander

KEY TIPS

Risk	Guidance
CBRN overlay exercise	Most technically specific block in the course — read TM-40E Chapter 6 the night before and know what fields the CBRN sensor feed exposes
Geographic CCIRs	Require correctly defined AOR boundaries in MSS — if your training environment does not have the AOR pre-loaded, ask the instructor before Day 1 how geographic CCIR boundaries are configured

Risk	Guidance
Threat reporting inject	When the inject hits, the correct response is: assume the gap is significant until proven otherwise, caveat everything affected, escalate immediately. Do not attempt to determine if the sector is "actually clear"
CCIR troubleshooting	Force protection CCIRs that monitor CBRN sensor status must be verified against the actual sensor feed update frequency — if sensors report every 30 minutes and the CCIR evaluates every 5 minutes, the CCIR will false-trigger 5 out of 6 cycles. Set CCIR evaluation frequency to match the source data refresh rate

ASSOCIATED EXERCISE AND EXAMS

Item	Reference
Practical Exercise	EX_40E (EXERCISE.md + ENVIRONMENT_SETUP.md) — `exercises/EX_40E_protection/`
Pre-course exam	EXAM_TM40E_PRE — `exercises/exams/EXAM_TM40E_PRE.md`
Post-course exam	EXAM_TM40E_POST — `exercises/exams/EXAM_TM40E_POST.md`

RELATED WFF TRACKS

SL 4E is one of six WFF tracks. All require SL 1, SL 2, and SL 3 as prerequisites.

Track	WFF	Audience
SL 4A	Intelligence	G2/S2 staff, targeting officers, all-source analysts
SL 4B	Fires	FSOs, FSEs, targeting officers, fires NCOs
SL 4C	Movement & Maneuver	G3/S3 staff, operations officers, maneuver planners
SL 4D	Sustainment	G4/S4 staff, logistics officers, supply chain managers
SL 4E	Protection	FP officers, CBRN officers, provost marshal staff
SL 4F	Mission Command	Battle captains, XOs, CDRs, MC-function staff

Personnel completing multiple WFF tracks do not repeat SL 1, SL 2, or SL 3. Enrollment is independent for each track.

USAREUR-AF Operational Data Team Syllabus SL 4E | Version 1.0 | March 2026