

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

COURSE SYLLABUS

SL 4A



COURSE SYLLABUS — SL 4A: INTELLIGENCE WARFIGHTING FUNCTION

Maven Smart System (MSS) — USAREUR-AF

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

DRAFT — NOT FOR OFFICIAL USE. FOR TRAINING PLANNING PURPOSES ONLY.

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

COURSE SYLLABUS — SL 4A: INTELLIGENCE WARFIGHTING FUNCTION

MAVEN SMART SYSTEM (MSS) — USAREUR-AF

Field	Detail
Level	SL 4A — Intelligence WFF Track
Duration	3 days (24 hours)
Prerequisites	SL 1, SL 2, SL 3 (Go evaluations on file); CONCEPTS_GUIDE_TM40A_INTELLIGENCE (required reading before Day 1)
Audience	G2/S2 staff, targeting officers, all-source analysts, personnel who configure or brief intelligence products in MSS at BCT echelon or above
Format	Instructor-led seminar + demonstration + tabletop exercise + practical evaluation
Location	MSS Training Environment (standard user access sufficient)

BLUF: SL 4A teaches G2/S2 staff to integrate MSS into intelligence and targeting workflows — configuring PIR alerts, maintaining intelligence COP layers, managing collection coverage visualization, and supporting targeting decisions with fused, attributed data. Course applies MSS capabilities to processes in FM 2-0 (Oct 2023) and ATP 2-01 (May 2023). No coding or pipeline experience required.

LEARNING OBJECTIVES

#	Objective
1	Configure and maintain intelligence data layers on the MSS COP — threat activity, NAIs/TAIs, FSCM overlays with intelligence annotations, IPB products — with explicit source attribution and currency timestamps
2	Build and configure PIR alerts with correct trigger conditions, data sources, and notification routing

#	Objective
3	Construct a collection status dashboard displaying NAI/TAI coverage, collection asset task status, and gaps against published PIRs
4	Produce an all-source intelligence summary product integrating multiple intelligence data layers with explicit sourcing and currency caveats
5	Support a targeting working group with an MSS targeting data product distinguishing confirmed from unconfirmed targets, with data-as-of timestamps and current BDA status
6	Identify and respond to collection gaps, data staleness events, and PIR alert failures before they propagate
7	Apply MSS OPSEC procedures for intelligence products: classification marking, distribution controls, export handling, and need-to-know verification
8	Distinguish reported intelligence (what MSS displays) from assessed intelligence (what the analyst judges) and communicate that distinction explicitly

PRE-COURSE CHECKLIST

Complete 5+ duty days before Day 1:

- Read CONCEPTS_GUIDE_TM40A_INTELLIGENCE in full — Day 1 builds directly on it; do not skip
- Confirm MSS training account is active
- Bring your unit's current PIR list (real or notional) — used during the Day 1 CCIR/PIR alert configuration exercise
- Review FM 2-0 (Oct 2023), Chapter 2 (Intelligence Operations) and ATP 2-01 (May 2023), Chapter 3 (Intelligence Support to Targeting)

DAILY SCHEDULE

Day 1 — IPB and COP Integration

Time	Block	Method	Content
0800–0900	1	Brief	Doctrinal context: FM 2-0 (Oct 2023), ATP 2-01 (May 2023); how MSS supports intelligence operations and the targeting cycle

Time	Block	Method	Content
0900–1100	2	Demo/Lab	Intelligence COP configuration: threat activity layers, NAI/TAI overlays, IPB products; data sources, display standards, freshness indicators
1100–1115	—	Break	
1115–1200	3	Lab	Verifying data currency: reading timestamps, tracing data source pipelines, identifying stale feeds; escalation path when a threat feed goes dark
1200–1300	—	Lunch	
1300–1500	4	Lab	PIR alert configuration: translating published PIR into MSS alert conditions; setting geographic and threshold triggers; routing notifications
1500–1515	—	Break	
1515–1700	5	Exercise	PIR scenario: given commander requirements and a sample intelligence dataset, configure 3 PIR alerts and verify they trigger correctly

Evening reading: TM-40A, Chapter 3 (Collection Management and Requirements) — focus on false-trigger diagnosis procedures.

Day 2 — Collection Management and Targeting Data Workflows

Time	Block	Method	Content
0800–0830	—	Review	Day 1 questions; PIR alert review — common threshold and boundary errors
0830–1030	6	Demo/Lab	Collection management visualization: collection status dashboard — NAI/TAI coverage, asset task status, collection gaps against PIRs
1030–1045	—	Break	
1045–1200	7	Lab	All-source fusion product: comparing multiple intelligence layers simultaneously; identifying corroboration and contradiction; building an INTSUM with sourcing attribution and currency caveats
1200–1300	—	Lunch	
1300–1500	8	Demo/Lab	Targeting data workflows: building a targeting product distinguishing confirmed from unconfirmed targets, with data-as-of timestamps and current BDA status

Time	Block	Method	Content
1500– 1515	—	Break	
1515– 1700	9	Exercise	Targeting product drill: build a targeting product from a provided intelligence dataset; evaluator reviews for timestamp, confirmed/unconfirmed distinction, BDA status, and OPSEC compliance

Evening reading: TM-40A, Chapter 8 (Intelligence Support to Targeting) and Chapter 4 (All-Source Analysis in MSS).

Day 3 — Practical Exercise

Time	Block	Method	Content
0800– 0900	10	Brief	OPSEC for intelligence products: classification marking, distribution controls, need-to-know verification, export handling
0900– 1015	11	Demo/L ab	Collection gap response: briefing a collection gap without presenting absence of reporting as absence of activity; MSS caveat procedures for unknown vs. clear NAI status
1015– 1030	—	Break	
1030– 1100	12	Brief	Practical exercise scenario brief; product standards checklist review; tabletop ground rules
1100– 1200	—	Prep	Practical exercise setup and planning time
1200– 1300	—	Lunch	
1300– 1700	13	Eval	Practical exercise: configure intelligence COP, set PIR alerts, build collection status dashboard, produce targeting product, respond to collection gap inject, apply OPSEC

REQUIRED READING

When	Reading
Before Day 1	CONCEPTS_GUIDE_TM40A_INTELLIGENCE (complete)
Before Day 1	FM 2-0 (Oct 2023), Ch 2 (Intelligence Operations) — review
Before Day 1	ATP 2-01 (May 2023), Ch 3 (Intelligence Support to Targeting) — review
Day 1 evening	TM-40A, Ch 3 (Collection Management and Requirements)
Day 2 evening	TM-40A, Ch 8 (Intelligence Support to Targeting)
Day 2 evening	TM-40A, Ch 4 (All-Source Analysis in MSS)
Day 3 (review)	TM-40A, Ch 7 (Intelligence Products and Dissemination) — skim before Day 3 brief

PRACTICAL EXERCISE

Scenario: You are the S2 section at a BCT headquarters during a force projection exercise. The commander requires a fully configured MSS intelligence COP with PIR alerts active, a collection status dashboard, and a targeting product before a targeting working group in four hours. At T+90 min, the evaluator injects a collection reporting gap: the primary collection feed for NAI TIGER stops reporting.

#	Task
1	Configure the intelligence COP with threat activity layers, NAI/TAI overlays, and IPB products; verify data currency for all displayed feeds
2	Build and validate 3 PIR alerts from the provided commander's PIR card
3	Construct the collection status dashboard showing NAI coverage, collection asset task status, and identified gaps
4	Build the targeting product with confirmed vs. unconfirmed target distinction, data-as-of timestamps, and current BDA status
5	Respond to the collection gap inject: identify affected COP elements, update the collection status dashboard, and brief the evaluator on what you will/will not brief to the targeting board
6	Apply OPSEC procedures to all intelligence products before simulated distribution

Go standard: Pass 5 of 6 tasks. No-Go on Task 2 (PIR alert configuration) or Task 5 (collection gap response) = automatic No-Go regardless of total score.

GO CRITERIA

Task	Hard Standard
PIR alerts	Correct trigger geometry AND correct data source — wrong data source fails even if geometry is correct
Collection gap inject	NAI TIGER must be characterized as unknown (not "clear") — briefing NAI TIGER as "clear" when the feed is down is an automatic No-Go on Task 5
Targeting product	Data-as-of timestamps on every target element AND explicit confirmed/unconfirmed status marking required

Function-Specific Go Criteria — Intelligence

Criterion	Standard
PIR alert thresholds	Thresholds must reference a specific intelligence indicator — "movement" is not a threshold; "vehicle count in NAI-7 exceeds 12" is
Confirmed vs. unconfirmed distinction	Targeting product must visually distinguish confirmed from unconfirmed targets using separate layers or a status field — not a verbal caveat
Collection gap characterization	When responding to the collection gap inject, trainee must state which PIR is affected, which collection asset is offline, and the time window of coverage gap — all three elements required for Go

KEY TIPS

Risk	Guidance
PIR alert configuration	A PIR must be tied to a specific data feed, geographic area or threshold, AND notification path — "report enemy movement in the AOR" is not a complete alert. Bring your unit's PIR list and think through configuration before Day 1
Collection gap inject	The failure mode is briefing NAI TIGER as "clear" when the feed is down. Correct answer: "NAI TIGER status unknown — collection gap." Caveat all commander products dependent on NAI TIGER coverage

Risk	Guidance
Targeting product	The evaluator will ask "How do you know this target is confirmed?" — if you cannot point to a confirmation source and BDA entry, that element fails
CCIR troubleshooting	PIR alerts that trigger on every data refresh are usually misconfigured as value-present rather than value-threshold alerts. Check the alert condition: does it trigger on any entry matching the PIR indicator, or on a count/status threshold? The latter is almost always what the commander needs

ASSOCIATED EXERCISE AND EXAMS

Item	Reference
Practical Exercise	EX_40A (EXERCISE.md + ENVIRONMENT_SETUP.md) — exercises/EX_40A_intelligence/
Pre-course exam	EXAM_TM40A_PRE — exercises/exams/EXAM_TM40A_PRE.md
Post-course exam	EXAM_TM40A_POST — exercises/exams/EXAM_TM40A_POST.md

RELATED WFF TRACKS

SL 4A 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 4A | Version 1.0 | March 2026

DRAFT