TECHNICAL MANUAL

SL 4A

USAREUR-AF

TM-40A — MAVEN SMART SYSTEM (MSS)

Specialist Course Manual

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

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

TM-40A — MAVEN SMART SYSTEM (MSS)

Forward: MSS integrates multi-INT data streams and intelligence cycle functions into a single enterprise environment. This chapter establishes how the Intelligence WFF operates within MSS, how MSS relates to legacy intel tools, and the access control framework governing intelligence workspaces. **Prereqs:** SL 1, Maven User; SL 2, Builder; SL 3, Advanced Builder; CONCEPTS_GUIDE_TM40A_INTELLIGENCE (required before beginning this manual). Familiarity with MSS workspace navigation and basic data querying (SL 1 standard) is assumed. No pipeline development or code experience required. *HQ USAREUR-AF · v1.0 · 2026 · DISTRIB: USG only · AUTH: C2DAO/UDRA v1.1*

WARNING: Releasing MSS intelligence products — including dashboards, exported datasets, and workspace screenshots — outside the originating classification domain without IMO and security manager review is a potential unauthorized disclosure. Verify handling requirements before any distribution. Classification of a compiled MSS product may exceed the classification of any individual source. CAUTION: MSS aggregates data from multiple sources with varying classification levels. Derived products combining SIGINT, HUMINT, and GEOINT data may be classified higher than any individual source. Do not determine product classification by the lowest-classified input. Apply derivative classification procedures (AR 380-5) before publishing or exporting any multi-source MSS product. NOTE: MSS is an intelligence enabler. The Intelligence cycle — Direction, Collection, Processing and Exploitation, Production, Dissemination — remains the doctrinal framework (FM 2-0). MSS accelerates and integrates the data layer within that cycle. Analytical judgment, source evaluation, and product integrity remain irreducibly human functions.

NOTE: FM 2-0 (October 2023), para 1-50, states: "MI professionals must develop data literacy skills... Until institutional training is adjusted to incorporate data literacy, intelligence professionals must build those skills through self-development." This TM directly addresses that doctrinal requirement. The tasks, procedures, and standards in SL 4A equip intelligence professionals with the data literacy competencies FM 2-0 identifies as essential to the modern intelligence enterprise.

CHAPTER 1 — OVERVIEW AND INTELLIGENCE FUNCTION IN MSS

BLUF: MSS integrates multi-INT data streams and intelligence cycle functions into a single enterprise environment. This chapter establishes how the Intelligence WFF operates within MSS, how MSS relates to legacy intel tools, and the access control framework governing intelligence workspaces.

1-1. Intelligence Specialist Manual

The Intelligence WFF facilitates understanding of the operational environment, enemy, terrain and weather, and civil considerations (ADP 2-0, para 1-1). It supports the commander's situational understanding and drives the targeting cycle, operations process, and risk assessment across all warfighting functions.

MSS does not change what intelligence does. It changes how intelligence data is stored, accessed, fused, and delivered to decision-makers. Before MSS, sections maintained separate databases and spreadsheet trackers, each keeping its own authoritative threat picture — reconciling those versions at the BUA consumed analyst time that should have been spent on analysis.

On MSS, datasets, workspaces, geospatial layers, and products share a common Ontology. The division G2 threat ORBAT is accessible — at the appropriate access level — by brigade S2 sections. Products are persistent, not ephemeral.

Table 1-0. MSS Value to Intelligence Practitioners

Value	Description
Speed of fusion	Multi-INT data queried against a common object model; MSS Ontology links allow direct cross-INT association without manual spreadsheet reconciliation
Persistence of products	Threat models remain accessible and updatable — not rebuilt from scratch before each briefing cycle
Cross-echelon visibility	Division G2 and brigade S2 sections share workspaces, reducing product cycle time and improving analytical coherence

1-2. The Intelligence Cycle in MSS

FM 2-0 defines the Intelligence cycle as Direction, Collection, Processing and Exploitation, Production, and Dissemination. MSS supports each phase without replacing the analytical and command functions within it.

Table 1-1. Intelligence Cycle Phase — MSS Function Cross-Reference

Cycle Phase	Doctrinal Function (FM 2-0)	MSS Function	Human Judgment Required
Direction	Establish PIRs, task collection, manage RFIs	PIR tracking workspace, RFI log, collection plan dashboard	Commander establishes CCIR; G2/S2 translates to PIRs
Collection	Execute collection against tasks	Collection asset status tracking, reporting feeds ingest	35H evaluates coverage and gaps

Cycle Phase	Doctrinal Function (FM 2-0)	MSS Function	Human Judgment Required
Processing and Exploitation	Convert raw data to usable form	Multi-INT dataset query, object fusion, pattern analysis	Source reliability and information credibility evaluation
Production	Create intelligence products	Workshop dashboards, Ontology-linked threat models, INTSUM templates	Analytical synthesis and finished intelligence assessment
Dissemination	Deliver products to consumers	Workspace sharing, read-only access grants, export products	Classification review; consumer need-to-know determination

NOTE: MSS accelerates each phase of the Intelligence cycle but does not automate analytical judgment. The analyst's assessment — "what does this data mean for the commander's decision?" — remains a human function at every phase.

1-2a. The Intelligence Process as Data Pipeline

The intelligence cycle maps directly to data platform operations. Intelligence professionals who understand this mapping can leverage MSS more effectively — the doctrinal process they already know is the same workflow the platform executes at the data layer.

Table 1-1a. Intelligence Process — Data Platform Operations Mapping (FM 2-0, Figure 1-2)

Intelligence Process Step	Data Platform Analog
Plan and Direct	Requirements definition, collection tasking
Collect and Process	Data ingestion, ETL/transforms
Produce (Analyze)	Analytical models, dashboards, reports
Disseminate and Integrate	Data publication, API endpoints, COP feeds

NOTE: This mapping is conceptual. The intelligence process involves human judgment at every step — particularly source evaluation, analytical synthesis, and classification determination — that the data platform does not replicate. The platform accelerates the data operations within each step; it does not replace the intelligence functions performed by trained analysts.

1-3. Intelligence Data Categories in MSS

MSS aggregates six primary intelligence categories. Each has different source origins, handling requirements, and Ontology representation. Analysts must understand these distinctions before fusing products across categories.

Table 1-2. Intelligence Categories in MSS

INT Category	Source Origin	MSS Representation	Handling Notes
GEOINT	NGA feeds, unit collections, commercial imagery	Geospatial layers, MGRS-linked objects, imagery overlays	Standard MSS access; coordinate with 35G for layer management
SIGINT	NSA feeds (where authorized), theater SIGINT assets	Activity datasets (metadata only at standard classification), event objects	Requires separate SIGINT workspace authorization; coordinate with G6
HUMINT	Unit collection teams, debriefs, source reporting	Contact report objects, source registry references, assessment datasets	Restricted workspace access; no source identifying information in MSS
OSINT	Open source aggregation, social media monitoring	Media event objects, geolocation-tagged reporting	Verify classification before entering; OSINT combined with other INT may be classified
MASINT	Technical collection feeds	Sensor data objects, geospatial signatures	Confirm access authorization before workspace creation
TECHINT	Exploitation reports, EPW technical data	Equipment object types, exploitation report objects	Link to ORBAT objects; coordinate with legal on EPW-related data

CAUTION: Not all INT categories are authorized in every MSS workspace. Confirm workspace classification level and data category authorization before loading SIGINT-derived data. Access to SIGINT data in MSS requires separate authorization beyond standard MSS access credentials. Contact the G6 and security manager before establishing a SIGINT workspace.

1-4. MSS vs. Legacy Intelligence Tools

MSS complements — it does not replace — legacy tools that remain authoritative for certain functions. Replacing these tools with MSS before appropriate data feeds and workflows are established will create gaps in intelligence production.

Table 1-3. MSS and Legacy Intel Tool Relationship

Legacy Tool	Primary Function	MSS Relationship	Action Required
DCGS-A	All-source analysis, production, national dissemination	MSS complements DCGS-A; DCGS-A remains primary for national-level dissemination	Establish DCGS-A to MSS reporting linkage through G6

Legacy Tool	Primary Function	MSS Relationship	Action Required
CPCE	Common Picture / COP at tactical level	MSS extends COP; CPCE remains authoritative for fire control integration	Coordinate COP display standards with S3 and fires cell
TIGR	HUMINT collection reporting, patrol debriefs	TIGR reports feed MSS HUMINT objects when linkage is established; TIGR remains primary submission tool	Coordinate TIGR-to-MSS feed with G6/MSS administrator
M3 (MIDB)	Military Intelligence integrated database — authoritative ORBAT	MSS threat objects supplement M3 for analytical use; M3 remains authoritative at theater level	Coordinate with theater G2 before creating MSS ORBAT
HOT-R	HUMINT operations tracker — source management	MSS collection tracking workspaces supplement HOT-R; HOT-R remains primary for source management	Never duplicate source registry data between HOT-R and MSS

NOTE: MSS does not replace DCGS-A, TIGR, HOT-R, or CPCE. It provides an enterprise data environment where their outputs can be integrated, visualized, and cross-referenced. Unit IMO and G6 must establish approved data feeds before MSS can display data from legacy systems. Build MSS workflows on top of these tools, not in place of them.

1-5. Authorization and Access Controls for Intelligence Workspaces

Intelligence workspaces require RBAC that exceeds the standard MSS access model. The intelligence section implements and maintains these controls — not the MSS administrator acting independently.

- All intelligence workspaces are initialized as restricted access. The workspace owner — G2/S2 section chief or designated IMO — must explicitly grant access to each user before access is permitted.
- Read-only access grants allow consumers to view dashboards and products without editing underlying data. Apply read-only access for all cross-functional sharing (fires, maneuver, sustainment) unless the user has a documented editing requirement.
- Write access to intelligence object types is restricted to designated analyst roles. Coordinate with the MSS administrator (35T or S6) to establish role assignment for each analyst position.
- Users must not add or modify HUMINT source references in MSS without supervisor authorization.
- Workspace audit logs are enabled by default for all intelligence workspaces. The G2 or S2 reviews access logs at each intelligence oversight cycle or as directed by the unit security manager.

Table 1-4. Intelligence MOS — MSS Role and Access Level Cross-Reference

MOS	Title	Standard MSS Role	Workspace Access Level	Restrictions
35A	MI Officer	Intelligence Analyst	Write — assigned workspaces	Coordinate with 35X before editing threat model objects
35D	All-Source Intel Officer	Senior Analyst	Write — all G2/S2 workspaces	Reviews products before dissemination
35F	Intelligence Analyst	Analyst	Write — assigned workspaces	HUMINT workspace restricted unless additional authorization granted
35G	Geospatial Intel Analyst	GEOINT Analyst	Write — GEOINT layers; Read — other intel workspaces	Coordinates targeting GEOINT with fires through 35D
35H	Collection Manager	Collection Manager	Write — collection plan workspace	No write access to finished intelligence products
35L	CI Agent	CI Analyst	Write — CI workspace; Read — all-source workspace	CI workspace restricted; need-to-know enforced per AR 381-10
35M	HUMINT Collector	HUMINT Analyst	Write — HUMINT workspace	HUMINT workspace restricted; source references by case number only
35N	SIGINT Analyst	SIGINT Analyst	Write — SIGINT workspace (separate authorization required)	Separate authorization required from theater SIGINT authority
35P	Cryptologic Linguist	Analyst Support	Read — assigned products	Write access requires explicit 35D or 35X authorization
35T	MI Systems Maintainer	MSS Administrator	Admin — configuration only; no analytic write	Does not access intelligence content without G2/S2 authorization
35X	Intel Senior Sergeant	Section Chief	Write — all intelligence workspaces	Responsible for access control enforcement and product quality
350F/350G	Strategic MI (FA)	Senior Analyst	Write — designated strategic workspace	Coordinates with theater G2 before creating strategic-level products

1-6. Intelligence Section MSS Accountability

MSS accountability is the G2/S2's responsibility. Assign the following functions to specific personnel by name and position — not as general section responsibilities.

Table 1-5. Required MSS Accountability Assignments

Function	Responsible	Responsibility
Workspace owner	Designated per workspace	Access controls, product currency, workspace health; first POC for access issues
Product curator	Designated per product	Currency and version control for each recurring product (INTSUM, I&W dashboard, threat model)
Collection management owner	35H	PIR status, collection asset assignments, RFI entries — no other section member modifies without 35H coordination
HUMINT/CI workspace authority	35X or designated officer	All access decisions for HUMINT and CI workspaces

Document assignments in the section SOP and brief all personnel at the start of each operational period or rotation.

1-7. MSS Setup Coordination Requirements

Complete all coordination below during pre-deployment preparation or exercise setup — not during an operational period.

Coordinate With	Actions Required
G6/MSS administrator (35T)	Workspace creation, data feed authorizations, RBAC role assignments, network access for all section personnel, audit log settings
Security manager and IMO	Classification levels per workspace, authorization for SIGINT/CI/HUMINT workspaces, export and handling procedures
Supported commander and S3/G3	Which products are shared via MSS access vs. traditional dissemination; standard product set required before each battle rhythm event

CHAPTER 2 — INTELLIGENCE PREPARATION OF THE BATTLEFIELD (IPOE) IN MSS

BLUF: IPOE is the foundational analytical process for understanding the operational environment and threat. MSS provides geospatial layers, terrain data, threat datasets, and collaborative workspace tools that directly support each of the four IPOE steps (ATP 2-01.3). IPOE in MSS is a continuous, living analytical product — not a one-time briefing.

2-1. IPOE Overview and MSS Integration

ATP 2-01.3 defines IPOE as a systematic, continuous process used by intelligence analysts to analyze the mission variables of threat, terrain and weather, and civil considerations in the operational environment (ATP 2-01.3, para 1-1). The four steps are: (1) Define the operational environment; (2) Describe effects of the environment on operations; (3) Evaluate the threat; (4) Determine threat courses of action.

IPOE is a continuous analytical process — not a one-time checklist. It updates as the situation develops, as collection reporting arrives, and as operations unfold.

In a traditional environment, rebuilding IPOE products is labor-intensive. MSS removes this constraint. Because IPOE objects are persistent, updating the picture means updating specific objects, not rebuilding products. A threat unit location update takes minutes; a new NAI links to existing PIRs immediately.

NOTE: IPOE products built in MSS must be validated against current intelligence before use in planning. A geospatial layer loaded six months ago may not reflect current terrain trafficability, population changes, or infrastructure modifications. Review layer currency and last-updated timestamps before briefing IPOE products to the commander. Stale IPOE presented as current is worse than no IPOE — it creates false confidence.

2-2. Step 1 — Define the Operational Environment in MSS

Step 1 establishes geographic boundaries, actors, and conditions defining the operational environment. In MSS, Step 1 produces the foundational workspace structure — boundaries, areas of interest, and civil considerations — that all subsequent IPOE steps reference.

Key products for Step 1 in MSS:

- AOR boundary layer (unit boundary, defining the area of analysis)
- Areas of interest (AI) — broader than the AOR; includes areas outside the unit boundary that could affect operations
- Named areas of interest (NAIs) — specific areas where collection is focused (linked to collection plan in Chapter 3)
- Adjacent unit boundaries (shared from higher/adjacent S2 sections)
- Civil considerations layer — population centers, key infrastructure, cultural sites

---

TASK BOX 2-1: Define Operational Environment in MSS

Conditions: The analyst has access to the unit's MSS IPOE workspace. Boundary datasets and AOR geospatial files have been received from higher headquarters in approved format (KML, KMZ, GeoJSON, or MGRS polygon). SL 1, SL 2, and SL 3 tasks are complete. MSS workspace has been established IAW Appendix E and the security manager has approved the classification level.

Standards: The analyst correctly loads and names the AOR boundary layer, identifies adjacent unit boundaries, and identifies all NAIs established in the current collection plan. All layers follow the naming convention in Appendix A. The Step 1 workspace structure is reviewable by the G2/S2 within 24 hours of workspace setup. Adjacent unit boundaries are confirmed against current operations order graphics.

Procedure:

1. Navigate to the IPOE workspace in MSS. If the workspace does not exist, submit a workspace creation request to the MSS administrator IAW Appendix E.
2. Open the Geospatial Layers panel. Load the AOR boundary file in approved format. Name the layer IAW Appendix A: `[UNIT]-AOR-BOUNDARY-[YYYYMMDD]`.
3. Load adjacent unit boundaries if available from the higher G2. Name each layer: `[ADJ-UNIT]-BOUNDARY-[YYYYMMDD]`. If boundaries are not yet received, create a placeholder layer noting "PENDING — awaiting higher G2 dissemination."
4. Create an Area of Interest (AI) boundary layer extending beyond the AOR to capture relevant adjacent areas. Name: `[UNIT]-AI-[YYYYMMDD]`.
5. Identify and mark all NAIs from the current collection plan. Create an NAI object for each, linked to the relevant PIR. Name each NAI: `NAI-[NUMBER]-[UNIT]-[YYYYMMDD]`.
6. Add operational area descriptors: population centers, road networks, key terrain identified by the GEOINT analyst (35G). Link terrain objects to the GEOINT workspace IAW Chapter 5.
7. Create the Civil Considerations layer group: major population centers (with estimated population if available), key infrastructure (bridges, power nodes, communication nodes), cultural and historical sites affecting operations.
8. Apply classification marking to the workspace before saving. Confirm with the security manager that the classification level is correct for the data loaded.
9. Brief workspace layout to the G2/S2 section chief for validation before sharing with adjacent sections.

2-3. Step 2 — Describe Environmental Effects in MSS

Step 2 analyzes how terrain, weather, and civil considerations affect friendly and threat operations. The analyst produces an assessment — not just a data display. MSS supports this through geospatial terrain layers, weather overlay integration, and named area datasets.

The 35G owns terrain-related MSS objects (see Chapter 5). The 35F synthesizes terrain, weather, and civil data into an effects assessment covering: - Terrain effects on friendly and threat mounted maneuver - Key avenues of approach and the echelon each supports - Weather effects on aviation, observation, and communications - Civil considerations presenting risk to operations or civilian protection obligations

This assessment is a text object linked to the Step 2 layer group — the analyst's product, not a data display.

Table 2-1. Environmental Effects Datasets in MSS

Dataset Type	Primary Owner	Layer Naming Convention	Review Cycle
Terrain trafficability	35G	`[UNIT]-TERRAIN-TRAFFICABILITY-[YYYYMMDD]`	Quarterly or after significant precipitation events
Key terrain	35F / 35G	`[UNIT]-KEY-TERRAIN-[YYYYMMDD]`	At each IPOE cycle update
Weather overlays	G2/S2 section	`[UNIT]-WEATHER-[YYYYMMDD]`	Daily when data feed is active
Civil considerations	35F (all-source)	`[UNIT]-CIVIL-CONSIDERATIONS-[YYYYMMDD]`	At each IPOE cycle update
Obstacles	35G / Engineers	`[UNIT]-OBSTACLES-[YYYYMMDD]`	At each IPOE cycle update; confirm with engineers
Aviation hazards	35G / Aviation	`[UNIT]-AVIATION-HAZARDS-[YYYYMMDD]`	Before aviation operations; coordinate with ADAM/BAE cell

2-4. Step 3 — Evaluate the Threat in MSS

Threat evaluation requires assessing threat capabilities, doctrine, and disposition — producing a coherent picture of what the threat can do in the operational environment.

Threat ORBAT. Maintained as linked Ontology objects: unit objects (type, echelon, location, condition estimate), equipment objects (type, quantity, location, capability), and aggregate personnel estimates. Objects link hierarchically — regiment to battalion to company — and to geospatial positions, enabling visual ORBAT display at any echelon.

Threat capability assessment. For each threat unit, the 35F/35D enters a capability assessment by warfighting function (fires, maneuver, sustainment, EW, air defense, engineer), each with an analyst-entered confidence rating.

Pattern of life. POL analysis tracks threat activity against time and location, establishing baselines and flagging deviations. See Chapter 4 for procedures.

CAUTION: Threat ORBAT data in MSS must be treated as a working analytical product, not an authoritative database. Verify threat data against current intelligence reporting before using ORBAT for planning or targeting. ORBAT products not reviewed within the last 72 hours in a high-activity environment should be marked "REVIEW REQUIRED — PERISHABILITY NOT CONFIRMED." A stale ORBAT presented as current status has directly contributed to intelligence failures in historical operations.

Table 2-2. Threat Evaluation Objects in MSS

Object Type	Key Data Fields	Owner	Update Trigger
Threat unit	Designation, echelon, type, MGRS location, confidence, last intel date	35F / 35D	Any new locating report or ORBAT update
Threat equipment	Type, quantity, location, condition estimate, source, confidence	35F / 35G	Exploitation report, imagery update, collection reporting
Activity event	Activity type, location, time, source, confidence, associated unit	35F	Any new event report or SALUTE
Pattern of life baseline	Activity type, frequency, location cluster, time window, deviation threshold	35F / 35D	Weekly minimum; update on significant deviation
Capability assessment	WFF-by-WFF assessment, confidence, supporting sources	35D	At each IPOE update cycle

2-5. Step 4 — Determine Threat COAs in MSS

Step 4 develops the MLCOA and MDCOA within the framework from Steps 1–3. MSS supports development and visualization — it does not generate COAs analytically. The determination is an analytical judgment based on doctrinal threat behavior, available intelligence, and terrain analysis.

COA overlays. Built as geospatial overlays: avenues of approach, objective areas, support-by-fire positions, assembly areas. Name and version each overlay: `[UNIT]-THREAT-COA-[MLCOA/MDCOA]-[YYYYMMDD]-V[N]`. Version on significant updates; archive previous versions.

COA indicator lists. Indicator objects identify specific activities that confirm or refute each COA. Each indicator links to a NAI (where observed) and to the collection plan (which asset is tasked). Indicator status (Observed / Not Observed / Ambiguous) updates as collection reporting arrives.

COA probability assessment. Each COA overlay carries an analyst-entered probability estimate reviewed at each IPOE update cycle.

TASK BOX 2-2: Build Threat COA Overlays and Indicator Lists in MSS

Conditions: IPOE Steps 1–3 are complete. Terrain analysis and threat ORBAT are loaded in the IPOE workspace. The 35D or senior 35F has completed the COA analysis and the G2/S2 section chief has approved the MLCOA and MDCOA determination.

Standards: MLCOA and MDCOA overlays are built with all required graphic control measures. Indicator list is complete with at least three indicators per COA. Each indicator is linked to a specific NAI and collection task. COA probability assessments are entered with supporting analytical rationale. The G2/S2 can brief the IPOE Step 4 product without additional analyst preparation.

Procedure:

1. Create the MLCOA overlay layer: `[UNIT]-THREAT-COA-MLCOA-[YYYYMMDD]-V1`. Add all graphic control measures: avenues of approach, probable attack positions, phase lines, objective areas.
2. Create the MDCOA overlay layer: `[UNIT]-THREAT-COA-MDCOA-[YYYYMMDD]-V1`. Same graphic requirements.
3. For each COA, add a text assessment object: probability estimate, key assumptions, key intelligence gaps that could change the assessment.
4. Create indicator objects for each COA. For each indicator: indicator text, associated COA, NAI linkage, collection asset assigned, and initial status ("Not Observed").
5. Link each indicator to the collection plan workspace (Chapter 3). Confirm the indicator is covered by an existing collection task.
6. Build the COA indicator dashboard (Chapter 4, Task Box 4-1). Ensure the dashboard is visible to the G2/S2 at all times.
7. Brief the completed COA overlays and indicator list to the G2/S2 section chief. Obtain approval before disseminating outside the intelligence section.
8. Establish the IPOE update cycle: at minimum, every 24 hours in a high-activity environment, or whenever a major indicator changes status.

2-6. IPOE Update Cycle Standards

Establish an IPOE update cycle as a section SOP. At minimum:

- Threat unit location objects: reviewed and confirmed or updated within 48 hours in steady state; within 12 hours during active operations.
- COA indicator list: reviewed against latest collection reporting at each battle rhythm event.
- Terrain and weather overlays: confirmed for currency at least weekly; weather data updated when available.
- Civil considerations layer: reviewed at each IPOE update cycle.

2-7. Collaborative IPOE with Adjacent S2 Sections

MSS workspace access grants enable sharing IPOE products with adjacent S2 sections and higher G2 without separate product dissemination. Submit workspace access requests through established channels to the adjacent section's S2 or G2 section chief. Request read access only to the specific workspaces needed. Provide read-only access — never write access — to adjacent or higher units reviewing the unit's IPOE workspace.

CHAPTER 3 — COLLECTION MANAGEMENT AND REQUIREMENTS

BLUF: Collection management converts intelligence requirements into collection tasks, synchronizes assets against requirements, monitors reporting, and identifies gaps. MSS provides the 35H with a platform to manage PIRs, the collection synchronization matrix, RFI tracking, and asset deconfliction. This chapter is the primary reference for the 35H but applies to all analysts within the collection management framework.

3-1. PIR and IR Management in MSS

PIRs are the commander's specific intelligence questions associated with CCIRs. IRs are additional requirements below the PIR threshold. Both are tracked in MSS.

PIR object structure. Each PIR links to: the CCIR it supports (coordinated with the S3 CCIR workspace per SL 4F), NAIs and indicators in the IPOE workspace, collection tasks and assigned assets, and reporting received in satisfaction or partial satisfaction.

PIR data entry requirements. PIR number (sequential within current OPORD), PIR text (as a question), associated CCIR number, supporting PIR if applicable, date established, expiration date or condition, and assigned priority.

PIR status values. Active / Partially Satisfied / Satisfied / Expired / Transferred to Higher. Update at each battle rhythm event.

NOTE: PIRs in MSS must be synchronized with the commander's current CCIR list. Before entering a new PIR, confirm it is on the CCIR list approved and signed by the commander. PIR tracking in MSS is a management tool — it does not constitute commander approval of the requirement. MSS PIR updates not reflected in the CCIR list create a gap between what the section is collecting against and what the commander has actually prioritized (FM 6-0).

3-2. Collection Synchronization Matrix in MSS

The CSM is the primary collection planning product, mapping PIRs to collection assets over time to provide visibility on coverage and gaps.

CSM structure. PIRs by priority (rows), time periods aligned to the battle rhythm (columns), and cells showing assigned collection asset, tasking authority, collection window, and report receipt status. A gap column highlights PIRs with no coverage.

TASK BOX 3-1: Establish and Maintain Collection Synchronization Matrix in MSS

Conditions: Commander has published CCIRs. PIRs are identified and approved by G2/S2 section chief. MSS collection management workspace is established with appropriate access controls. Collection assets have been tasked through appropriate channels.

Standards: All active PIRs are entered in MSS with complete object data. All tasked collection assets are linked to their assigned PIR with collection windows and tasking authority documented. The CSM dashboard is readable and current. Collection gaps are identified and visible. RFI log is maintained with status updated within 4 hours of any status change. G2/S2 can review collection coverage and gaps without additional analyst preparation.

Procedure:

1. Navigate to the collection management workspace. Verify access controls: only the 35H and G2/S2 section chief have write access to PIR and collection assignment objects.
2. Enter each PIR as an object. Confirm all required data fields are complete: PIR number, PIR text, priority, CCIR linkage, NAI assignment, expiration condition, and indicators of satisfaction.
3. For each PIR, link the assigned collection assets: asset type, tasking authority, collection window, and reporting due date.
4. Build the CSM dashboard: PIR rows, time period columns, cells showing assigned asset and current status (Tasked / Collecting / Reported / Gap).
5. Identify and flag all collection gaps: PIRs with no asset assigned, or assets that have not reported within the expected reporting window. Brief gaps to the G2/S2 at the next collection management update.
6. Create the RFI log (Appendix B template). Link all active RFIs to their associated PIR.
7. At each battle rhythm event, review the CSM with the G2/S2. Update asset assignments and PIR status based on reporting received.
8. When a PIR is satisfied, update status to "Satisfied" and record the satisfying report reference. Archive satisfied PIR objects — do not delete.

3-3. RFI Workflow in MSS

RFIs from subordinate or adjacent units are tracked in MSS to prevent duplication, ensure timely response, and maintain collection deconfliction.

RFI log fields. RFI number (IAW Appendix B), requesting unit, RFI text, associated PIR, priority (Urgent/High/Routine), due DTG, assigned analyst or collection asset, response status, and response summary on closure.

RFI submission. Units submit through the established channel per unit SOP. The 35H enters the RFI in MSS and assigns for action. The CSM dashboard tracks all open RFIs by priority and due date. Overdue RFIs are flagged for G2/S2 attention.

CAUTION: MSS RFI tracking does not replace the formal RFI submission process required by unit SOP and higher headquarters guidance. MSS is the tracking tool — the formal submission goes through the approved channel. Entering an RFI in MSS does not constitute submission to the collection node. The 35H must confirm through direct coordination that the RFI has been formally received by the tasking authority.

3-4. CCIR Linkage to MSS Dashboards

The intelligence section coordinates with the S3/Mission Command workspace (SL 4F) to ensure PIR-derived CCIR components appear on the commander's unified CCIR dashboard alongside FFIR components. Coordination requires: establishing a shared workspace or dashboard panel both sections can update, defining which intelligence products populate the CCIR display, and confirming data-as-of timestamps for each element.

NOTE: The CCIR dashboard must display data-as-of timestamps for each CCIR element. A PIR displayed as "Not Observed" is only meaningful if the timestamp confirms the collection cycle is current. Brief the commander on the last collection update cycle before presenting CCIR status at any decision point. A PIR with no recent collection reporting is a gap — not a "Not Observed" finding.

3-5. Collection Gap Reporting Standards

Collection gaps are not administrative problems — they are intelligence failures in progress. An unreported gap is a gap the commander doesn't know exists. The 35H must identify gaps, report them clearly, and track resolution.

Collection gap report format. When briefing gaps to the G2/S2, the 35H provides: PIR number and text; reason for the gap (no asset, asset not reporting, tasking lapsed); gap duration; recommended resolution (retask organic asset, submit RFI, or acknowledge as unresolvable); and impact on the IPOE assessment if the gap persists.

Documenting unresolvable gaps. When a gap cannot be resolved, the G2/S2 formally documents it and notifies the commander. An undisclosed collection gap is an intelligence failure — the commander must know what PIRs remain unanswered and why.

3-6. Collection Asset Deconfliction

When multiple sections, echelons, or units task the same collection assets against overlapping areas, the 35H uses the collection management workspace to identify conflicts and coordinate resolution.

Deconfliction process. Review the tasking matrix for each asset. If an asset appears tasked to multiple simultaneous requirements, coordinate with the tasking authority to establish priority and sequencing. Document the deconfliction in the collection management workspace and brief the resolution to the

G2/S2.

Echelon deconfliction. When collection assets are tasked by both organic (S2) and higher HQ (G2), confirm the tasking authority hierarchy. Organic tasking belongs to the lowest echelon with the requirement. Higher HQ tasking takes precedence unless the S2 has coordinated an exception with the higher G2.

Deconfliction documentation. Document all deconfliction decisions: which assets were in conflict, which PIR took priority, who made the priority decision, and what collection was rescheduled or deferred. This prevents recurrence and supports lessons learned.

Asset availability tracking. When a collection asset is unavailable — maintenance, recall, or comms loss — update asset status in the collection management workspace immediately. The MSS dashboard must reflect the actual reason for each gap so the G2/S2 can make an informed recommendation.

Cross-echelon asset visibility. When organic assets are insufficient, coordinate with the higher G2 collection manager for augmentation. Before requesting, confirm through MSS: which PIRs are uncovered, what organic assets are available, why organic coverage is insufficient, and what collection window is required. A documented gap request in MSS is more likely to be prioritized and easier to track to completion.

CHAPTER 4 — ALL-SOURCE ANALYSIS IN MSS

BLUF: All-source analysis fuses multiple intelligence categories into coherent assessments supporting the commander's decisions. MSS enables multi-INT fusion through Ontology-linked objects, time-series analysis, link analysis, and Indications and Warning monitoring. This chapter is the primary reference for 35F and 35D analysts.

4-1. Multi-INT Fusion in MSS

All-source analysis combines GEOINT, SIGINT, HUMINT, OSINT, and other INT categories to produce assessments no single source can support. MSS enables fusion through linked Ontology objects — a HUMINT report, a geospatial observation, and a SIGINT event can be associated within the same analytical workspace.

Standard all-source analytical workflow:

1. **Query.** The analyst queries relevant object types across INT categories for the area and time window of interest.
2. **Association.** The analyst links related objects from different INT sources — same time window, same geographic cluster, or same subject entity.

3. **Corroboration assessment.** Do these sources genuinely corroborate each other, or do they appear to agree because they reflect the same underlying observation seen from different angles?
4. **Assessment.** The analyst forms an analytical judgment: what does the corroborated picture indicate about threat intent, capability, or likely COA?
5. **Product.** The analyst updates or creates a finished intelligence product reflecting the assessment (Chapter 7).

NOTE: MSS enables multi-INT linkage but does not evaluate source credibility or information reliability. Analysts must apply standard source and information reliability ratings (FM 2-22.3, Appendix H) to all intelligence reporting before incorporating into fused products. An MSS object with no source reliability rating is an unvalidated data point — not intelligence.

4-2. Pattern of Life Analysis

POL analysis establishes behavioral baselines for threat actors, facilities, and areas of interest. Deviations from baseline indicate changed threat posture, operational preparation, or emerging activity.

Building a POL baseline. Query activity events over a defined time period and geographic area, establishing frequency, timing, and location patterns. Minimum baseline: 14 days — sufficient to capture normal variation.

Deviation detection. Configure a dashboard panel to flag deviations: activity above or below baseline threshold, outside the normal location cluster, or outside the normal timing window. Deviations require investigation — not automatic conclusions.

Table 4-1. Pattern of Life Analysis Parameters

Parameter	Description	Recommended Value
Baseline window	Time period for establishing normal pattern	14–30 days minimum; adjust for operational tempo
Deviation threshold (frequency)	% change from baseline frequency that triggers flag	25% above or below baseline
Geographic deviation	Distance from normal cluster triggering a flag	500m for point activity; 2km for area activity
Timing deviation	Hours outside normal window triggering a flag	±2 hours from baseline timing pattern
Update cycle	How often the analyst updates the baseline	Weekly in steady state; after each significant deviation
NAI linkage	Which NAI the POL baseline supports	Required — must support a specific PIR through a linked NAI

4-3. SIGACT Analysis and Event Management

SIGACTs are the primary record of battlefield events in MSS. Every SIGACT entered feeds POL analysis, threat ORBAT assessment, and I&W indicator tracking. SIGACT quality determines analytical quality.

SIGACT entry standard. Every SIGACT must include: event type (approved taxonomy only — no ad hoc types), location (10-digit MGRS), time (Zulu), associated threat unit (linked to ORBAT object where identified), source (HUMINT / SIGINT / GEOINT / observer / report), and source reliability rating applied at entry — not retroactively.

SIGACT taxonomy consistency. Event type taxonomy must be consistent across the section and synchronized with higher HQ taxonomy where applicable. Inconsistent typing prevents meaningful pattern analysis. The 35X establishes and enforces SIGACT taxonomy as a section standard.

Periodic SIGACT analysis. See Section 4-2 on Pattern of Life Analysis for the analytical use of SIGACT data. SIGACT entry is a data function; SIGACT analysis is an analytical function. Both are required.

4-4. Link Analysis and Network Mapping

Link analysis identifies relationships between entities — organizations, locations, equipment, events. In MSS, it is performed by querying and visualizing Ontology object relationships to map threat networks, supply chains, and command relationships.

Network map structure. Nodes (entities) and edges (relationships). Node types: organizations, locations, equipment sets, events. Edge types: command relationship, logistics link, financial link, known association, observed co-location. Each edge carries: relationship type, source reference, confidence level, and date of last confirmation.

CAUTION: Persons of interest in a network map must be referenced by designated case or contact numbers — never by full name, physical description, or identifying information — in MSS unless the workspace has been specifically authorized for that data category. Coordinate with the CI section (35L) and the unit legal advisor before creating person-linked objects in MSS. Creating a person-linked object without this authorization may violate AR 381-10 and Privacy Act requirements.

4-5. Indications and Warning Monitoring

I&W monitoring tracks threat indicators against established warning conditions. MSS supports I&W through indicator objects linked to COA overlays (Chapter 2), collection assets (Chapter 3), and reporting datasets.

TASK BOX 4-1: Build and Maintain I&W Dashboard in MSS

Conditions: Threat COA analysis (Chapter 2) is complete. MLCOA and MDCOA indicators are identified and reviewed by the G2/S2 section chief. All-source workspace is established with appropriate access controls. Collection plan covers the NAIs associated with each indicator.

Standards: All warning indicators are entered as MSS objects with current status, source linkage, and last-updated timestamp. I&W dashboard is accessible to the G2/S2 at all times without additional analyst preparation. Indicator status is updated within 2 hours of receipt of relevant reporting. Dashboard clearly distinguishes indicators by associated COA and warning level.

Procedure:

1. Open the all-source workspace. Navigate to the I&W indicator panel.
2. Verify all COA indicators from the IPOE workspace (Chapter 2) are linked to the I&W panel. Use Ontology links — do not duplicate objects. Duplicate objects create version control problems when indicators are updated.
3. For each indicator, confirm: indicator text, associated COA (MLCOA or MDCOA), geographic area of observation (NAI linkage), reporting source type, and current status.
4. Add any supplemental warning indicators established by the G2/S2 beyond the IPOE COA indicators.
5. Build the I&W summary dashboard panel: grouped by warning level (Alert / Watch / Elevated / Normal), with indicator status, last-updated timestamp, and source reference for each "Observed" finding.
6. Establish the section SOP for I&W monitoring outside battle rhythm events. Designate a watch officer or on-call analyst responsible for updating indicator status when new reporting arrives.
7. When an indicator changes status to "Observed," immediately notify the G2/S2 and update the dashboard. Document: reporting source, confidence level, analyst assessment of significance, and time of update.
8. When enough indicators have shifted to support a COA determination change, prepare an I&W update brief for the G2/S2. Do not change the IPOE COA assessment without G2/S2 review and approval.

4-6. Building and Maintaining Threat Models

A threat model in MSS is a persistent analytical product linking threat ORBAT objects, capability assessments, POL data, and COA analysis into a single queryable representation of the threat in the AOR.

Threat model structure: - Unit objects linked to location, equipment, echelon, and condition - Capability assessments by warfighting function with confidence ratings and source citations - Activity pattern objects linked from pattern of life analysis - COA objects linked from IPOE COA overlays - Confidence ratings on every assessment element with last-confirmed date

Threat model review cycle. The G2/S2 section chief reviews the threat model at each battle rhythm event. Before any commander briefing, the analyst confirms: (1) all unit location objects reviewed within the last 48 hours; (2) all capability assessments reviewed within the last seven days; (3) all COA indicator statuses current.

NOTE: Threat models in MSS are analytical products, not authoritative assessments. They represent the unit S2/G2 analytical judgment as of the last update. Brief the last-updated date and analyst confidence level when presenting threat model outputs to the commander. An unreviewed threat model can mislead a commander as badly as no threat model at all.

4-7. Threat Model Maintenance Cycle Standards

The following maintenance standards apply to all intelligence sections using MSS.

Weekly threat model review (minimum). At least once per week, the section chief or designated 35D reviews the threat model in its entirety:

- Verify all threat unit location objects have been reviewed and confirmed or updated within the last 48 hours
- Verify all capability assessments have been reviewed within the last 7 days; update where new collection changes the assessment
- Confirm all pattern of life baseline objects are current and any recent deviations have been assessed
- Verify all COA assessments and probability estimates reflect the current intelligence picture

Trigger-based threat model updates. The following events trigger an immediate threat model update, regardless of the weekly review cycle:

- New imagery showing significant ORBAT change (unit repositioning, major equipment arrival/departure)
- HUMINT report confirming or contradicting existing threat disposition assessment
- Collection of a COA indicator that changes the MLCOA/MDCOA probability assessment
- Significant threat activity event (contact, strike, observed preparation activity)
- Receipt of updated higher headquarters ORBAT that changes the theater threat picture

Threat model update documentation. When updating a threat model object, enter in the object notes: what changed, what reporting drove the change, and the analyst's confidence in the updated assessment. This documentation creates an analytical audit trail and supports intelligence continuity across personnel rotations.

4-8. Source and Information Reliability Standards

All reporting objects entered in MSS must carry: source reliability rating (A–F per FM 2-22.3, Appendix H), information credibility rating (1–6), date of information (not entry date), and collection method.

Source reliability ratings (FM 2-22.3): A — Completely reliable; B — Usually reliable; C — Fairly reliable; D — Not usually reliable; E — Unreliable; F — Reliability cannot be judged.

Information credibility ratings: 1 — Confirmed by other sources; 2 — Probably true; 3 — Possibly true; 4 — Doubtful; 5 — Improbable; 6 — Truth cannot be judged.

WARNING: Skipping source and information reliability rating in MSS reporting objects removes the primary quality control mechanism from the intelligence pipeline. Products built from unrated sources cannot carry valid confidence ratings. The G2/S2 must enforce reliability rating as a non-negotiable standard for any report entered into the all-source workspace.

CHAPTER 5 — GEOSPATIAL INTELLIGENCE (GEOINT) IN MSS

BLUF: GEOINT provides the spatial foundation for all MSS intelligence analysis. The 35G analyst owns geospatial layers in the intelligence workspace. This chapter covers imagery exploitation, layer management, NAI construction, GIS integration, MGRS-based analysis, and targeting support.

5-1. The 35G Analyst Role in MSS

The 35G manages the geospatial data layer in MSS — the spatial foundation for all other intelligence analysis. Key MSS functions:

- Upload and manage geospatial layers (terrain, imagery overlays, infrastructure data, weather)
- Establish and maintain NAI objects with accurate geospatial boundaries linked to the collection plan
- Perform MGRS-based analysis for threat location and targeting
- Integrate KML/KMZ products from higher HQ and adjacent units
- Maintain the temporal archive of geospatial products for historical comparison
- Support targeting with geospatial target packages (Chapter 8)

Errors in geospatial data propagate through the entire IPOE and targeting picture.

5-2. Imagery Exploitation and Layer Management

Imagery in MSS is managed as geospatial overlays linked to timestamped ingest records.

Imagery upload. Upload through the Geospatial Layer upload function in the GEOINT workspace. Name each layer: `[UNIT]-IMAGERY-[AREA]-[YYYYMMDD]`. Record the collection date (not the upload date) in layer metadata — the collection date is the operationally relevant currency indicator.

Exploitation annotation. After upload, annotate with exploitation findings: identified threat equipment (linked to ORBAT objects where possible), activity observations, facility changes, terrain features of interest. Each annotation: object type, location (MGRS), confidence level, analyst initials.

Layer archiving. Layers older than 30 days not actively referenced in current analysis move to the archive layer group. Archived layers remain queryable. Never delete without G2/S2 authorization.

TASK BOX 5-1: Upload and Register Geospatial Layer in MSS

Conditions: Geospatial data file is received in approved format (KML, KMZ, GeoJSON, or GeoTIFF). GEOINT workspace is established with appropriate access controls. Analyst has write access to the GEOINT layer group. Classification of the file has been confirmed.

Standards: Layer is uploaded with correct naming convention, imagery collection date recorded in metadata, classification marking applied, and layer linked to relevant NAI or IPOE object. Exploitation annotations entered for all identified threat activity within 4 hours of upload during operational periods. Section chief confirms upload within 24 hours.

Procedure:

1. Verify file format and classification marking before upload. Do not upload files without confirmed classification designation. If uncertain, contact the security manager before proceeding.
2. Navigate to the GEOINT workspace, Geospatial Layers panel.
3. Upload the file. Enter the naming convention from Appendix A during the upload process.
4. In layer metadata: enter the imagery collection date or data collection date (not upload date), source, and classification marking.
5. Link the layer to the relevant NAI, IPOE overlay, or threat object.
6. Conduct imagery exploitation. For each identified item of intelligence value, create an annotation object: object type, MGRS location, confidence, and source.
7. Notify the G2/S2 section chief and relevant analysts that a new layer is available and exploitation is complete.
8. If this layer supersedes a previous version, move the previous version to the archive layer group immediately. Note the relationship in both layers' metadata.

5-3. MGRS-Based Analysis Standards

All geospatial analysis in MSS uses MGRS as the primary coordinate reference.

Coordinate precision standards: - Point objects (threat locations, activity events, weapons systems): 10-digit MGRS (10-meter precision) - Area objects (NAIs, boundaries): MGRS polygon with 8-digit precision minimum for all vertices - Large-area objects (AOR-scale): 6-digit MGRS is acceptable for

rough-scale display

WARNING: Incorrect MGRS coordinates in MSS can directly affect targeting products and fire mission execution. Before confirming any target location object in the targeting workspace, verify coordinates against primary source reporting and at least one corroborating source. A single-digit MGRS error can displace a target by hundreds of meters. Verify grid zone designator, 100,000m square identifier, and easting/northing sequence for every target coordinate entered in MSS.

5-4. Named Area of Interest (NAI) Management

NAIs are specific geographic areas where collection is focused to confirm or deny threat COAs. In MSS, NAIs are Ontology objects with geospatial boundaries linked to: the supporting PIR, assigned collection assets, indicators monitored within the NAI, and the threat COA the NAI assesses.

NAI creation. Create each NAI as a geospatial boundary polygon. Apply MGRS coordinates for all boundary vertices. Name: `NAI-[NUMBER]-[UNIT]-[YYYYMMDD]`. At each collection plan update, review: Is this NAI linked to an active PIR? Is the collection asset still tasked? Is the boundary still correct? Archive (do not delete) NAIs no longer linked to active PIRs.

5-5. KML/KMZ Integration and GIS Layer Management

Higher HQ GEOINT products are typically provided in KML, KMZ, or GeoJSON formats. Upload received files to a designated "received products" layer group — separate from unit-produced layers. Label with originating unit, product date, and classification to prevent confusion with own analytical products.

5-6. Supporting Targeting with Geospatial Products

The 35G's primary targeting contributions:

- Target location object with MGRS coordinates and source reference
- Imagery overlay confirming target description, terrain, and adjacent civilian infrastructure
- Geospatial CDE buffer zone display layer (the 35G provides the display layer only; CDE analysis is performed by JAG and the targeting officer)
- Post-strike imagery overlay for BDA comparison against pre-strike baseline

Confirm coordinate reference system and datum with the fires cell before sharing targeting geospatial products. Inconsistent MGRS formats between intelligence and fires create targeting errors.

CHAPTER 6 — HUMINT AND COUNTERINTELLIGENCE IN MSS

BLUF: HUMINT and CI operations involve the most sensitive data in the intelligence function. MSS provides management tools for contact report tracking, CI screening data, and source registry management — with strict access controls and handling requirements. The 35M and 35L are the primary users of Chapter 6.

6-1. SIGINT Analyst Workflow in MSS

The 35N operates in a separate, specially authorized workspace. Before beginning any MSS activity, the SIGINT workspace must be authorized by the theater SIGINT authority, the G6, and the unit security manager — separate from and in addition to standard MSS access credentials.

35N MSS functions (authorized workspace only):

- Enter SIGINT activity events: activity type (metadata only at standard classification), location (MGRS), time, associated unit or network (where determinable), and confidence rating
- Link SIGINT events to ORBAT objects where activity can be attributed to a specific threat unit
- Link SIGINT events to pattern of life objects where temporal and geographic patterns are assessed
- Provide SIGINT-derived indicators to the all-source workspace for COA indicator tracking

SIGINT data entry restrictions. The 35N must apply SIGINT-specific classification and handling markings to all SIGINT objects entered in MSS. When in doubt about whether specific SIGINT content can be entered in the MSS environment, coordinate with the theater SIGINT authority before entry — not after.

WARNING: Improper entry of SIGINT data into MSS — including content that reveals collection methods, sources, or capabilities beyond what the workspace authorization permits — is a SIGINT security violation. The consequences include compromise of collection capabilities that are not replaceable on the battlefield timelines. When uncertain, do not enter. Seek authorization first.

6-3. HUMINT Collector Operational Workflow in MSS

The 35M uses MSS to manage contact reports, link reports to collection requirements, and support all-source fusion. MSS does not replace TIGR or HOT-R — it provides the analytical management layer.

Contact report tracking. Each completed contact (debrief, elicitation, liaison, screening) generates a contact report. In MSS, contact report objects include: report date, collection date (if different), location (MGRS), collection category, associated PIR, reporting status (submitted to TIGR: Y/N), and link to all-source workspace.

Contact reports do not contain source identifying information. Only the designated case number or contact designator appears in the MSS contact report object. Full report content remains in TIGR or the authorized HUMINT management system.

WARNING: Personally identifiable information (PII) and source identifying information — including full names, physical descriptors, contact locations, and meeting details — must never be entered in MSS contact report objects. MSS is not authorized for source identifying data unless specifically cleared for that data category by the security manager and IMO. Non-compliance creates unauthorized disclosure risk for human sources. This is a life-safety requirement.

6-4. Source Registry Management in MSS

The source registry maintains a reference-only record of active sources by case number. MSS records source existence (by case number) and links to associated reporting and collection requirements. Source biographic, contact, and access data remain in HOT-R — not MSS.

Source registry structure. Each source object: case number, associated PIRs, reporting history (links to contact report objects), reliability rating, and access areas (geographic or organizational areas where the source has demonstrated collection access).

Source registry access. Restricted to: the 35M case handler(s), the 35L CI agent, the G2/S2 section chief, and the supporting HUMINT staff officer. The MSS administrator does not access the source registry without explicit G2/S2 authorization. Monthly audit by the G2/S2.

6-5. CI Screening Data Management

The 35L uses MSS to manage CI screening records, link screening results to threat assessments, and coordinate CI-derived threat indicators with the all-source section.

Screening record objects. CI screening record objects include: screening event date, location (MGRS), associated operational context, result category (no derogatory / minor derogatory / significant derogatory / referral), and linkage to threat assessment if applicable. No screened individual's identifying information appears in MSS. Reference by event designator only.

CI threat indicator linkage. When a CI screening event produces a threat indicator — hostile intelligence activity, penetration attempt, surveillance detection — the 35L creates a linked indicator object in the all-source workspace, stripped of identifying information, for inclusion in the I&W picture. Indicators suggesting penetration of intelligence collection activities are reported immediately to the G2/S2 and unit security manager — not entered in MSS first.

6-6. Privacy Act and Need-to-Know Controls

All HUMINT and CI data in MSS is subject to the Privacy Act of 1974 and AR 381-10.

Need-to-know. Access to any workspace containing HUMINT or CI objects requires documented need-to-know established before access is granted. Rank and clearance do not substitute. The G2/S2 section chief makes all need-to-know determinations for HUMINT and CI workspaces.

Training. All personnel with HUMINT or CI workspace access must complete AR 381-10 training prior to access.

Audit review. Audit logs are reviewed monthly by the G2/S2 section chief or designated representative. Any access anomaly is reported to the unit security manager.

CAUTION: MSS access controls are a technical safeguard — they are not a substitute for proper personnel handling training. Access controls prevent unauthorized access from outside the approved group. They do not prevent mishandling by authorized users. All personnel with HUMINT and CI workspace access must be briefed on workspace-specific handling requirements before access is granted, not after.

CHAPTER 7 — INTELLIGENCE PRODUCTS AND DISSEMINATION

BLUF: Intelligence products are the output of the intelligence cycle. MSS enables persistent, updatable products delivered via dashboard and supports controlled dissemination through access grants. This chapter covers all standard intelligence product types, MSS implementation, dissemination standards, and classification handling.

7-1. Intelligence Product Types in MSS

Table 7-1. Intelligence Product Types — MSS Implementation Reference

Product Type	Doctrinal Purpose	MSS Format	Primary Owner	Typical Cycle
INTSUM	Current threat and environment summary for the commander	Workshop dashboard + formatted text export	35F / 35D	Daily; or per battle rhythm event
INTREP	Specific event or significant development report	Report object linked to source reporting	35F	On significant event
SALUTE Report	Field observation — Size, Activity, Location, Unit, Time, Equipment	SALUTE object template in collection workspace	Any analyst / observer	On observation

Product Type	Doctrinal Purpose	MSS Format	Primary Owner	Typical Cycle
Decision Support Template (DST)	GO/NO-GO criteria overlaid on COA graphic	Geospatial overlay + decision matrix dashboard	35D / 35F	Per planning cycle
Threat Assessment	Formal assessment of threat capability, intent, and COA	Workshop dashboard product	35D	Per OPORD or FRAGO cycle
I&W Product	Current indicator status and warning level	I&W dashboard (Chapter 4)	35F / 35D	Continuous; briefed at battle rhythm events
GEOINT Product	Imagery and terrain analysis with exploitation annotations	Geospatial overlay + annotated imagery	35G	On imagery receipt or terrain update
PIR/Collection Status	Collection coverage against PIRs	Collection synchronization matrix dashboard	35H	Per collection cycle
Target Package	Target nomination, supporting intelligence, CDE inputs	Targeting workspace product (Chapter 8)	35F / 35G (with fires)	Per targeting cycle

7-2. INTSUM Standards in MSS

The INTSUM is built as a Workshop dashboard displaying: current threat assessment, I&W status, significant events in the last period, and intelligence outlook for the next period.

INTSUM dashboard required elements:

- Classification marking prominently displayed at top
- Period covered (from date/time to date/time)
- Threat assessment summary (current MLCOA assessment, I&W status, threat posture trend)
- Significant activity (events from the reporting period linked to reporting objects)
- Collection summary (PIR coverage status, gaps, RFIs answered this period)
- Intelligence outlook (key decision points anticipated, planned collection)
- Data-as-of timestamp for each automated data element
- Analyst assessment text — written by 35D/35F, not auto-generated
- Analyst name, position, and G2/S2 approval signature

Analyst assessment text is not optional. A dashboard displaying only data is not an INTSUM. The analyst must write a current assessment of the threat situation, the significance of recent activity, and the outlook for the next period.

7-3. MSS Dashboard as Intelligence Product

MSS Workshop dashboards are live intelligence products that update continuously from source data. The analyst's role shifts from product generator to product curator — ensuring data quality, analytical assessments, and confidence ratings remain current.

Product currency standards. Every intelligence dashboard must display: - Product title and classification marking - Owning section and analyst position - Data-as-of timestamp (automated; analyst verifies currency before each briefing) - Analyst confidence rating for each major assessment element - Last-reviewed date (analyst-entered at each battle rhythm event confirming the product has been reviewed and the assessment is current — distinct from the auto-updated data timestamp)

7-4. Dissemination via MSS Workspace Access

MSS dissemination uses workspace access grants. The intelligence product remains in MSS; consumers receive read access. This is the preferred method — it maintains classification control, enables in-place updates, and provides an audit trail.

Dissemination access levels: - **Read-only:** Consumer can view dashboards; cannot edit. Appropriate for all cross-functional sharing. - **Comment:** Consumer can add annotations; cannot edit objects. Appropriate for adjacent intelligence sections providing analytical coordination. - **Write:** Reserved for the producing intelligence section. Not granted for dissemination.

Pre-dissemination checklist. Before granting access to any intelligence product workspace:

1. Confirm consumer clearance level meets or exceeds product classification.
2. Confirm consumer has documented need-to-know.
3. Obtain G2/S2 section chief approval for the access grant.
4. Log the access grant: consumer name, position, access level, workspace, date granted, approval authority.
5. Set an access review date (next personnel rotation or 90 days, whichever is sooner).

7-5. Classification Handling Within MSS

MSS product classification follows derivative classification rules (AR 380-5, E.O. 13526). A compiled MSS product may be classified higher than any individual source.

Derivative classification procedure: 1. List all source classifications used in the product. 2. Assess whether the combination reveals information warranting higher classification. 3. Apply the highest classification warranted by the combination. 4. Apply required markings: overall classification top and bottom; portion markings on each section. 5. Include "Derived From:" citation listing source workspaces and their classifications. 6. Include "Declassify On:" date or event if determinable.

WARNING: Exporting MSS intelligence products to external media — USB, printed documents, email attachments — requires IMO and security manager review before export. Treat all exported intelligence products as requiring formal classification determination before distribution. Unauthorized exports are reportable security incidents.

7-6. Product Naming and Version Control

All intelligence products follow Appendix A naming conventions. Version numbers increment on substantive analytical updates only — not routine data refreshes.

Version increment triggers: Significant change in threat COA assessment; new PIR satisfied or added; major ORBAT update; change in I&W warning level.

CHAPTER 8 — INTELLIGENCE SUPPORT TO TARGETING

BLUF: Intelligence drives targeting. MSS provides the shared data environment enabling D3A execution, HVT/HPT tracking, and BDA monitoring. Intelligence-fires integration through MSS requires coordinated workspace access and clear data ownership established before operations begin. This chapter covers the intelligence role in the targeting cycle.

8-1. D3A Methodology in MSS

D3A (Decide-Detect-Deliver-Assess, FM 3-60) is the targeting framework. Intelligence supports three of the four phases directly.

Decide — Target development. Intelligence identifies target sets tied to the commander's objectives, conducts target value analysis, builds HVT/HPT nominations, and creates target objects in MSS linked to the threat ORBAT and IPOE.

Detect — Target detection and tracking. Collection management (Chapter 3) and I&W monitoring (Chapter 4) enable detection. When an HVT/HPT is located, the analyst updates the target object with current location, confidence level, and source reference — immediately visible to fires through the shared targeting workspace.

Assess — BDA. BDA is tracked as a linked object to the original target, enabling direct before/after comparison of pre-strike intelligence with post-strike assessment.

NOTE: Intelligence does not own targeting. The targeting process is led by the targeting officer under the fires cell. Intelligence provides a critical input — target development, detection, and BDA collection. The targeting decision and attack authorization belong to the commander and targeting officer, not the G2/S2.

8-2. HVT/HPT List Management in MSS

TASK BOX 8-1: Establish and Maintain HVT/HPT Tracker in MSS

Conditions: Commander has approved the HVT/HPT list. Targeting officer has established the targeting workspace and coordinated access with the intelligence section. Classification controls are confirmed on the targeting workspace. Intelligence and fires sections have completed the pre-operation targeting checklist (Appendix D).

Standards: All HVT/HPT entries are entered as target objects with complete data fields. Target location is updated within 2 hours of receipt of a new locating report. Confidence ratings are current and reflect the most recent intelligence. Targeting officer and G2/S2 can access current HVT/HPT status without analyst preparation. BDA tracking object templates are prepared in advance for each nominated target.

Procedure:

1. Coordinate with the targeting officer to confirm write access for the intelligence section to the intelligence columns of the targeting workspace.
2. Enter each HVT/HPT as a target object: target designation number, target category, associated commander's objective, description (capability-based), last known location (MGRS), location confidence level (High/Medium/Low), source of location intelligence, date of last intelligence.
3. Link each target object to relevant all-source intelligence: ORBAT unit linkage, associated pattern of life object, relevant GEOINT layer.
4. Build the target status dashboard panel: all active HVT/HPTs, last known location, date of last intelligence, confidence level, and current status (Unknown / Collection Tasked / Tracked / Located / Nominated / Approved / Struck / BDA Pending / Assessment Complete).
5. Establish the update SOP with the targeting officer: when a new locating report is received, who updates the target object and within what time limit? Standard: 2 hours from receipt during active targeting cycles.
6. Prepare BDA tracking object templates for each nominated target. Confirm the BDA collection requirements (which assets will observe effects, required reporting format).
7. After a strike, update target status to "Struck" with strike date/time group. Activate the BDA tracking object. Link BDA reporting to the target object as it is received.

8-3. Target Synchronization Matrix in MSS

The TSM synchronizes targets, collection, attack systems, and timing. In MSS, it is a Workshop dashboard maintained jointly by intelligence, fires, and the targeting officer.

TSM data ownership: - Intelligence (35H): collection column — which assets are tasked against each target - Intelligence (35F/35D): intelligence assessment column — current location, confidence, target analysis - Fires (FECC): attack column — assigned attack system, munitions, windows - Targeting officer: overall TSM review, approval, and re-attack determination

TSM review cycle. The targeting officer and G2/S2 review the TSM at each targeting board. Stale data must be updated or flagged as a collection gap immediately.

8-4. Intelligence-Fires Integration Access Coordination

The most common cause of intelligence-fires integration failure is late access coordination — workspace access established during a targeting event rather than before. Complete the Appendix D checklist at the beginning of each operational period. Validate that both sections have correct access levels and confirm by test login before operations begin.

8-5. BDA Tracking in MSS

BDA categories tracked in MSS:

- **Physical damage.** Structural damage from imagery or ground reporting. The 35G assesses using post-strike imagery compared against pre-strike baseline.
- **Functional damage.** Target no longer capable of performing its function. Assessed from reporting, signals, or pattern of life changes indicating disrupted operations.
- **System damage.** Network or organization degraded. Assessed from all-source analysis of network behavior following the strike.

BDA confidence standards. Each BDA assessment: confirmed (observed effects with high-confidence source), probable (indirect indicators supporting assessment), possible (assessment based primarily on inference). The targeting officer uses the BDA confidence level to determine whether re-attack is warranted.

CHAPTER 9 — ECHELON-SPECIFIC INTELLIGENCE OPERATIONS

BLUF: Intelligence operations and MSS use vary substantially by echelon. This chapter provides echelon-specific guidance from BCT S2 through theater G2.

9-1. BCT S2 Section

The BCT S2 is responsible for the brigade commander's IPOE, collection management for the MI Company, and intelligence production for the brigade TOC.

MSS functions: IPOE workspace (Chapter 2), collection management workspace (Chapter 3), all-source analysis workspace (Chapter 4), targeting workspace (Chapter 8), and INTSUM/threat assessment products for the brigade TOC.

MI Company integration. The BCT's MI Company provides HUMINT collection teams, a SIGINT platoon, and a GEOINT section. Establish collection reporting feeds and workspace access during pre-deployment setup — not in contact.

Table 9-1. BCT S2 MSS Workspace Set

Workspace	Owner	Primary Write Users	Read Access Granted To	Minimum Classification
IPOE	S2 NCOIC (35X)	S2 analyst section	S3, fires cell, XO	SECRET
Collection Management	35H	35H, S2 officer	G2/S2 section chief	SECRET
All-Source Analysis	35D / senior 35F	S2 analyst section	None without G2/S2 approval	SECRET
HUMINT	35M section chief	35M, S2 officer	35L, section chief only	SECRET//NOFORN minimum
GEOINT	35G	35G	S2 section (read)	SECRET
Targeting	Targeting officer (collocated)	FSE/FECC, 35F, 35G	Brigade commander, XO (read)	SECRET

9-2. Division G2

The Division G2 provides intelligence support to the division commander and enables subordinate BCTs with production capability exceeding organic BCT capacity.

MSS functions: IPOE workspace covering the division AOR (shared read with BCT S2 sections), ACE workspace aggregating BCT reporting with corps intelligence, division targeting workspace, and strategic collection management coordinating with the MI brigade.

Division-to-BCT product flow. Division G2 pushes products to BCT S2 sections via MSS read access. Division ACE receives read access to BCT all-source workspaces for collection reporting aggregation. Write access does not cross echelon boundaries.

9-3. Corps G2

The Corps G2 operates an all-source production cell, a SIGINT cell, and a collection management section integrating theater, national, and allied intelligence.

MSS functions: Multi-division ORBAT workspace, long-range collection synchronization across the corps AOR, corps targeting workspace, and allied/partner nation intelligence coordination workspaces authorized under applicable MOUs.

SIGINT cell workspace. The corps SIGINT cell requires separate workspace authorization beyond standard MSS credentials. Coordinate with the MSS administrator, G6, and theater SIGINT authority. Do not create a SIGINT workspace without all authorizations confirmed in writing.

9-4. Theater/Army G2 (USAREUR-AF)

At the USAREUR-AF theater level, the G2 coordinates with INSCOM and national-level agencies for strategic intelligence production.

Theater MSS functions: Theater ORBAT workspace (most current and authoritative in the USAREUR-AF enterprise), national-level feed integration workspaces, allied intelligence coordination workspaces (established under bilateral/multilateral sharing agreements), and theater threat assessment production providing the baseline picture for all subordinate echelons.

INSCOM support. When INSCOM provides data feeds into MSS, the theater G2 establishes controlled access workspaces. Corps and division G2 sections receive read access to authorized products — not direct access to the INSCOM feed workspace.

CHAPTER 10 — DEGRADED AND CONTESTED OPERATIONS

BLUF: Intelligence operations do not pause when MSS is unavailable. This chapter establishes procedures for maintaining minimum essential intelligence functions without MSS, protecting intelligence data during degraded operations, and reconstituting the intelligence workspace after outage.

10-1. Intelligence Operations During MSS Degradation

MSS degradation may result from network outage, cyber incident, CP displacement, or adversary action. In USAREUR-AF's high-intensity conflict environment, MSS degradation is a planning assumption, not a contingency. The section must maintain minimum essential intelligence functions at all times.

Minimum essential intelligence functions without MSS: - IPOE products — existing printed products (Step 1–4 overlays, threat ORBAT table, COA indicators) - PIR and collection plan — maintained in hard-copy matrix - INTSUM — produced from DCGS-A or formatted report template - I&W monitoring —

manual indicator tracking against printed indicator list - SALUTE reporting — radio or SIPR message formatted report - Target tracking — hard-copy HVT/HPT list with voice/message coordination with fires cell

10-2. Pre-Operation Backup Product Generation

Before deployment or each major exercise, the S2 section generates a current set of printed backup products from MSS. These are maintained in a classified secure container and updated at each significant IPOE change.

Table 10-1. Required Printed Backup Products

Product	Content	Update Trigger	Storage
IPOE terrain overlay map	Key terrain, NAIs, obstacles, AOR boundary	At each IPOE update	Classified container
Threat ORBAT table	Unit designations, locations, confidence, last intel date	Within 48 hours of significant ORBAT change	Classified container
COA overlays (printed map)	MLCOA and MDCOA on printed map	At each COA revision	Classified container
Indicator list	All active indicators with current status	At each battle rhythm event	Classified container
Active RFI log	Open RFIs, priority, and due dates	Daily	Classified container
HVT/HPT list	Active targets with last known location	Within 2 hours of significant targeting update	Classified container

NOTE: Printed backup products are the minimum floor for continued intelligence operations during MSS outage. They are not a substitute for MSS when MSS is operational — they may not reflect the current analytical picture. Do not use printed products when MSS is available.

10-3. PACE Plan Integration

The intelligence section contributes PACE requirements to the unit PACE plan. Coordinate with the G6/S6 to ensure intelligence PACE requirements are resourced.

Table 10-2. Intelligence PACE Requirements

Tier	Network/System	Intelligence Capability	Access Method
Primary	MSS via unit SIPR network	Full MSS intelligence capability	Standard MSS login

Tier	Network/System	Intelligence Capability	Access Method
Alternate	DCGS-A via SIPRNET	All-source analysis, INTSUM production, collection management	DCGS-A terminal
Contingency	SIPR email + pre-printed products	Formatted INTSUM via email; manual indicator tracking	Secure email
Emergency	Radio / courier + printed products	SALUTE via radio; manual INTSUM delivery	Printed products; courier

When transitioning between PACE tiers, the S2 section chief notifies the G2 and the MSS administrator. All intelligence products generated on alternate means must be reconciled with MSS upon restoration.

10-4. Protecting Intelligence Data During CP Displacement

Displacement intelligence protection checklist: - ☐ All printed classified products and working documents inventoried and loaded in classified container before march order - ☐ Classified containers sealed and manifested before departure - ☐ DCGS-A and intelligence terminals cleared of classified data IAW unit SOP - ☐ S2 section confirmed with G6 that network continuity will be maintained or alternate MSS access plan is coordinated - ☐ On arrival at new CP, MSS access verified by test login before declaring intelligence function operational

10-5. Reconstitution After Outage

TASK BOX 10-1: MSS Intelligence Workspace Reconstitution After Outage

Conditions: MSS has been restored after an outage of more than 4 hours. Intelligence operations continued using alternate means during the outage. The G6 or MSS administrator has confirmed that MSS is operational and workspace data integrity has been verified.

Standards: All offline intelligence reporting is entered in MSS within 4 hours of restoration. All workspace objects are updated to reflect the current situation. The G2/S2 is briefed on the current intelligence picture within 2 hours of MSS restoration. The outage duration and analytical gaps are documented in the workspace log.

Procedure:

1. Verify MSS workspace integrity before entering new data. Confirm with the MSS administrator that no data corruption occurred during the outage.
2. Enter all SALUTE reports and event objects generated during the outage as backdated objects — use the actual event time, not the entry time. Note in each object that it was entered post-outage.
3. Update I&W indicator statuses for all changes that occurred during the outage period.

4. Update the threat ORBAT with any confirmed location or status changes from offline reporting.
5. Update the collection plan with any new taskings, RFIs processed, or collection reporting received during the outage.
6. Update the target tracker with any new locating reports, BDA reporting, or target status changes.
7. Notify the G2/S2 that MSS is restored and reconstitution is complete. Brief a summary of what occurred during the outage and the current intelligence picture.
8. Document the outage duration, analytical gaps created, and any reporting not captured during the outage in the workspace log. This documentation supports future PACE plan refinement.

APPENDIX A — INTELLIGENCE-SPECIFIC MSS NAMING CONVENTIONS

A-1. General Principles

All intelligence objects and workspaces follow a hierarchical naming convention identifying owning unit, product type, subject, date, and version.

Base format: `[UNIT]-[TYPE]-[SUBJECT/AREA]-[YYYYMMDD]-V[N]`

- `[UNIT]`: Unit abbreviation (e.g., 1BCT, 1ID, V-CORPS)
- `[TYPE]`: Product type abbreviation (see tables below)
- `[SUBJECT/AREA]`: Geographic area or subject (abbreviated, no spaces)
- `[YYYYMMDD]`: Date established or last major version update
- `V[N]`: Version number (omit on initial creation; add V2 on first revision)

A-2. Workspace Naming

Table A-1. Workspace Naming Conventions

Workspace Type	Naming Format	Example
IPOE	`[UNIT]-IPOE-[YYYYMMDD]`	`1BCT-IPOE-20260315`
All-source analysis	`[UNIT]-ALLSOURCE-[YYYYMMDD]`	`1ID-ALLSOURCE-20260315`
Collection management	`[UNIT]-COLLMGMT-[YYYYMMDD]`	`1BCT-COLLMGMT-20260315`
GEOINT	`[UNIT]-GEOINT-[YYYYMMDD]`	`1BCT-GEOINT-20260315`
HUMINT	`[UNIT]-HUMINT-[YYYYMMDD]`	`1BCT-HUMINT-20260315`

Workspace Type	Naming Format	Example
CI	`[UNIT]-CI-[YYYYMMDD]`	`1BCT-CI-20260315`
Targeting	`[UNIT]-TARGETING-[YYYYMMDD]`	`1BCT-TARGETING-20260315`
I&W	`[UNIT]-IW-[YYYYMMDD]`	`1BCT-IW-20260315`
Network analysis	`[UNIT]-NETANALYSIS-[YYYYMMDD]`	`1BCT-NETANALYSIS-20260315`

A-3. Object Naming

Table A-2. Intelligence Object Naming Conventions

Object Type	Naming Format	Example
NAI	`NAI-[NUMBER]-[UNIT]-[YYYYMMDD]`	`NAI-001-1BCT-20260315`
PIR	`PIR-[NUMBER]-[UNIT]-[YYYYMMDD]`	`PIR-1-1BCT-20260315`
IR	`IR-[NUMBER]-[UNIT]-[YYYYMMDD]`	`IR-5-1BCT-20260315`
Threat unit	`[THREAT DESIGNATION]-[ECHELON]-[YYYYMMDD]`	`XX-COMB-ARMS-RGT-20260315`
Activity event	`EVT-[YYYYMMDDHHMMZ]-[AREA]`	`EVT-202603151430Z-NAI001`
COA overlay	`[UNIT]-THREAT-COA-[MLCOA/MDCOA]-[YYYYMMDD]-V[N]`	`1BCT-THREAT-COA-MLCOA-20260315-V2`
Geospatial layer	`[UNIT]-[LAYER TYPE]-[AREA]-[YYYYMMDD]`	`1BCT-TERRAIN-TRAFFICABILITY-NORTH-20260315`
Intelligence product	`[UNIT]-[PRODUCT]-[SUBJECT]-[YYYYMMDD]-V[N]`	`1BCT-INTSUM-NORTHERN-20260315-V1`
Contact report	`CR-[CASE NUMBER]-[YYYYMMDD]`	`CR-BCT-001-20260315`
Target	`TGT-[NUMBER]-[UNIT]-[YYYYMMDD]`	`TGT-001-1BCT-20260315`
RFI	`RFI-[YYYY]-[NNN]-[UNIT]`	`RFI-2026-001-1BCT`

A-4. Archive and Version Control

When superseding a product version: (1) Create the new version with incremented version number. (2) Move the previous version to the archive layer group immediately. (3) Note in the new version's metadata that it supersedes the previous version and note the archive location. Never overwrite a previous version.

APPENDIX B — RFI TEMPLATE AND TRACKING STANDARD

B-1. RFI Object Data Fields

Table B-1. Required RFI Data Fields in MSS

Field	Content	Required?
RFI Number	`[UNIT]-RFI-[YYYY]-[NNN]` (sequential)	Yes
Requesting Unit	Full unit designation and requesting section	Yes
Requesting POC	Name and contact information	Yes
RFI Text	Specific information required, phrased as a question	Yes
Associated PIR	PIR number this RFI supports, if applicable	Conditional
Priority	Urgent / High / Routine	Yes
Date/Time Submitted	Date and time group when submitted	Yes
Requested Due Date/Time	Date/time group when response is needed	Yes
Assigned To	Analyst or collection asset responsible for response	Yes
Status	Open / In Progress / Answered / Closed / Transferred	Yes
Response Summary	Brief summary of information provided	Required on answer
Response Date/Time	Date/time group when response was provided	Required on answer
Close Date/Time	Date/time group when RFI was closed	Required on close

B-2. RFI Priority Definitions and Response Standards

Priority	Definition	Required Response Timeframe
Urgent	Supports imminent decision; delay affects ongoing operations	As soon as possible; not to exceed 4 hours
High	Supports near-term planning; significant operational impact if delayed	Within 24 hours
Routine	Supports future planning or background understanding	Within 72 hours or by requested due date

B-3. RFI Tracking Dashboard

The 35H maintains an RFI tracking dashboard displaying: all open RFIs by priority and due date, age of each RFI in days, overdue RFIs (past due date) flagged in a separate panel, and RFI response rate metric for the current reporting period. The G2/S2 reviews the RFI tracking dashboard at each battle rhythm event.

APPENDIX C — CLASSIFICATION AND HANDLING QUICK REFERENCE

C-1. Classification Levels and MSS Access Requirements

Table C-1. Classification Levels in MSS Intelligence Workspaces

Level	MSS Access Requirement	Key Restrictions	Handling Notes
CUI	Standard MSS access + documented need-to-know	No distribution outside authorized users without IMO review	Mark all exports CUI
SECRET	SECRET clearance + need-to-know	Standard SECRET handling; no foreign national access without authorization	Standard SECRET handling
SECRET // NOFORN	SECRET clearance + NOFORN determination + need-to-know	Not releasable to partner nations under any circumstances	Verify before sharing with allied liaison officers
SECRET // REL TO [COUNTRY]	SECRET clearance + bilateral MOU authorization + need-to-know	Releasable only to named countries per current MOU	Confirm MOU is current before any release
TS/SCI	TS/SCI clearance + specific compartment access + need-to-know	Separate workspace required	Contact security manager before creating TS/SCI workspace

C-2. Derivative Classification Quick Reference

When compiling an MSS product from multiple sources:

1. List all source classifications.
2. Apply the highest individual source classification as the starting point.
3. Assess whether the combination reveals information warranting higher classification.

4. Apply combination classification if warranted — upward classify if required; do not over-classify.
5. Add required markings: "Derived From: [sources]"; "Declassify On: [event or date]."
6. Confirm with security manager if uncertain.

C-3. Export Handling Requirements

Export Method	Required Actions
Printed document	Apply classification markings top and bottom; handle per AR 380-5
Email attachment (SIPR)	Classify per document; confirm recipient clearance and need-to-know
USB/removable media	Requires IMO approval; must be authorized media; log the export with date, recipient, and classification
Dashboard screenshot	Classify as CUI minimum; confirm full classification before distribution
Briefing slide	Apply classification markings; G2/S2 approval before briefing outside section

APPENDIX D — INTELLIGENCE-FIRES INTEGRATION CHECKLIST

Complete at the beginning of each operational period or exercise. Review at each personnel rotation.

D-1. Pre-Operations Setup

- ☐ Targeting workspace established and named IAW Appendix A
- ☐ G2 intelligence section write access granted to intelligence columns of targeting workspace
- ☐ Fires section (FECC) write access granted to attack and effects columns
- ☐ Both sections confirmed read access to the other's columns
- ☐ Targeting officer confirmed full workspace access
- ☐ HVT/HPT list entered as MSS target objects with complete data fields
- ☐ IPOE COA overlays linked to targeting workspace
- ☐ BDA tracking object templates prepared for each nominated target
- ☐ Classification controls confirmed on targeting workspace
- ☐ Coordinate reference system (MGRS) and datum confirmed between intelligence and fires sections
- ☐ All access confirmed by test login before declaring operational

D-2. During Operations

- ☐ HVT/HPT location updated within 2 hours of new locating report receipt
- ☐ New target nominations added to targeting workspace within SOP timeline
- ☐ Targeting board decisions reflected as object status updates
- ☐ Collection tasking linked to each target nomination for the detection phase
- ☐ Strike execution logged in target object by fires section
- ☐ BDA collection tasked for each executed strike
- ☐ BDA reporting linked to target object within 24 hours of receipt

D-3. Post-Strike BDA

- ☐ Physical damage BDA entered with source, confidence, and date
- ☐ Functional damage assessment entered
- ☐ System damage assessment entered (if applicable)
- ☐ Target status updated: struck / re-attack required / target neutralized / BDA pending
- ☐ ORBAT updated to reflect assessed damage if capability impact is confirmed
- ☐ Targeting officer notified of BDA assessment for re-attack determination
- ☐ BDA results filed in workspace log for targeting cycle lessons learned

APPENDIX E — MSS WORKSPACE SETUP FOR S2 SECTION

E-1. Initial Workspace Request Format

Submit workspace creation requests to the MSS administrator (35T or S6 designee) with G2/S2 section chief approval.

Table E-1. Workspace Creation Request Fields

Field	Information Required
Requesting section	Full unit designation and section (e.g., 1BCT S2)
Workspace type	IPOE / All-Source / Collection Management / GEOINT / HUMINT / CI / Targeting
Required classification	CUI / SECRET / SECRET//NOFORN / TS-SCI
Security manager approval	Name and date of security manager approval for the classification level

Field	Information Required
Workspace owner	Name, position, and unit of the workspace owner
Initial access list	Full name, position, clearance level, and access role for each initial user
Special handling requirements	Additional data category restrictions (SIGINT authorization, HUMINT, CI)
Required operational date	When the workspace must be available and operational

E-2. Minimum Workspace Setup Checklist

Complete before first operational use:

All Intelligence Workspaces: - ☐ All workspaces created and named IAW Appendix A - ☐ All section personnel access confirmed by test login before the operational period - ☐ Classification markings applied to each workspace; security manager review complete - ☐ Audit logs enabled and confirmed with MSS administrator - ☐ Backup product generation schedule established

IPOE Workspace: - ☐ AOR boundary layer loaded, named, classified - ☐ NAIs created and linked to PIRs - ☐ COA overlay templates prepared and named - ☐ Key terrain and obstacle layers loaded - ☐ Adjacent unit read access coordinated and confirmed

Collection Management Workspace: - ☐ All active PIRs entered with complete data fields - ☐ Collection synchronization matrix built and readable - ☐ RFI log template configured - ☐ 35H write access and G2/S2 read access confirmed

All-Source Analysis Workspace: - ☐ I&W indicator panel configured with all COA indicators linked from IPOE workspace - ☐ Threat ORBAT objects created and linked to geospatial positions - ☐ Pattern of life baseline objects created for priority NAIs - ☐ INTSUM dashboard template built and confirmed readable by G2/S2

Targeting Workspace: - ☐ Intelligence-fires access coordination complete per Appendix D checklist - ☐ HVT/HPT list entered - ☐ BDA tracking object templates prepared

HUMINT Workspace: - ☐ Access restricted to 35M case handlers, 35L, and G2/S2 section chief only - ☐ Source registry templates configured (case number reference only) - ☐ Contact report object templates configured with case-number-only fields - ☐ Security manager briefed on workspace handling requirements

Degraded Operations: - ☐ Initial backup products generated and stored in classified container - ☐ PACE plan intelligence requirements documented and briefed to G6/S6 - ☐ DCGS-A available and operational as alternate means

GLOSSARY

ACE. Analytical Control Element. The all-source production element at division level.

AOR. Area of Responsibility. The geographic area for which a commander is assigned authority and responsibility.

BDA. Battle Damage Assessment. The assessment of physical, functional, and system damage resulting from military action (FM 3-60).

CCIR. Commander's Critical Information Requirements. Information the commander identifies as critical for timely decision-making; includes PIRs and FFIRs (FM 6-0).

CI. Counterintelligence. Activity and information to identify, deceive, exploit, disrupt, or protect against espionage, sabotage, and related threats (ADP 2-0).

COA. Course of Action. A plan accomplishing the mission.

CPCE. Command Post Computing Environment. The tactical common operating picture system.

CSM. Collection Synchronization Matrix. A product mapping PIRs to collection assets over time.

D3A. Decide, Detect, Deliver, Assess. The targeting methodology (FM 3-60).

DCGS-A. Distributed Common Ground System — Army. The Army's primary intelligence processing, exploitation, and dissemination system.

DST. Decision Support Template. A product integrating COA overlays with decision criteria and timing.

FECC. Fires and Effects Coordination Cell.

FFIR. Friendly Force Information Requirements. Information the commander needs about friendly forces (FM 6-0).

GEOINT. Geospatial Intelligence. Intelligence derived from imagery and geospatial information.

HOT-R. HUMINT Operations Tracker — Redesigned. The primary Army HUMINT source management system.

HPT. High Payoff Target. A target whose loss significantly contributes to success of the friendly COA.

HUMINT. Human Intelligence. Intelligence derived from human sources (FM 2-22.3).

HVT. High Value Target. A target the enemy commander requires for successful mission accomplishment.

I&W. Indications and Warning. Intelligence activities to detect and report time-sensitive developments.

IMO. Information Management Officer. The unit officer responsible for information management and handling policy.

INSCOM. U.S. Army Intelligence and Security Command.

INTSUM. Intelligence Summary. A periodic report providing a current assessment of the operational environment and threat.

INTREP. Intelligence Report. A formatted report on a specific intelligence event or development.

IPOE. Intelligence Preparation of the Battlefield. A systematic, continuous process analyzing mission variables of threat, terrain, weather, and civil considerations (ATP 2-01.3).

IR. Information Requirement. A requirement for information supporting intelligence production.

MASINT. Measurement and Signature Intelligence. Intelligence from technical sensors detecting and characterizing physical attributes.

MDCOA. Most Dangerous Course of Action. The threat COA with the most severe potential impact on friendly operations.

MGRS. Military Grid Reference System. The geocoordinate standard for NATO military applications.

MI. Military Intelligence.

MLCOA. Most Likely Course of Action. The threat COA assessed as most probable given current intelligence.

NAI. Named Area of Interest. A geographic area where collection is focused to answer a specific intelligence requirement.

ORBAT. Order of Battle. The identification, strength, command structure, and disposition of threat forces.

OSINT. Open-Source Intelligence. Intelligence derived from publicly available information.

PACE. Primary, Alternate, Contingency, Emergency. The communications and operational continuity plan.

PIR. Priority Intelligence Requirement. The commander's most critical intelligence question, associated with a CCIR.

POL. Pattern of Life. Analysis of routine activities and behaviors to establish baselines and detect deviations.

RBAC. Role-Based Access Control. The MSS access control model assigning permissions by role.

RFI. Request for Information. A time-sensitive requirement for specific intelligence.

SALUTE. Size, Activity, Location, Unit, Time, Equipment. The standard field observation report format.

SIGINT. Signals Intelligence. Intelligence derived from communications and electronic signals.

TECHINT. Technical Intelligence. Intelligence from exploitation of foreign materiel.

TIGR. Tactical Ground Reporting system. The primary system for HUMINT reporting at the tactical level.

TSM. Target Synchronization Matrix. A product synchronizing targets, collection, attack assets, and timing.

APPENDIX F — INTELLIGENCE SYNCHRONIZATION MEETING SUPPORT PROCEDURES

The Intelligence Synchronization Meeting (ISM) is the battle rhythm event where the G2/S2 presents the intelligence picture, reviews collection coverage, and coordinates intelligence requirements. MSS provides the data foundation for the ISM. This appendix establishes standards for MSS-based ISM support.

F-1. ISM Preparation — MSS Verification Requirements

Complete the following before each ISM. The G2/S2 section chief verifies completion before the meeting begins.

Intelligence Picture Verification: - ☐ INTSUM dashboard reviewed; analyst assessment text is current (last reviewed within 24 hours) - ☐ Threat unit location objects reviewed for currency within 48 hours (within 12 hours during active operations) - ☐ COA indicator statuses updated against latest collection reporting - ☐ I&W dashboard status reviewed; changes from last ISM documented with analyst assessment - ☐ Pattern of life: significant deviations from baseline in the last reporting period are identified and assessed

Collection Coverage Review: - ☐ Collection synchronization matrix current: all PIRs and asset assignments reflect the current collection plan - ☐ Collection gaps identified: which PIRs have no coverage? Which have partial coverage? - ☐ RFI tracker reviewed: overdue RFIs flagged; new RFIs since last ISM captured - ☐ Collection reporting received this period: which PIRs did it satisfy or partially satisfy? - ☐ New tasking issued this period: are collection asset assignments updated in the CSM?

Product Status: - ☐ All scheduled products for this ISM are complete and available in MSS - ☐ Data-as-of timestamps verified for all dashboard products being briefed - ☐ Classification markings confirmed on all products being briefed - ☐ Previous ISM action items closed or updated in MSS

F-2. ISM Briefing Flow and MSS Products

Table F-1. ISM Briefing Flow — MSS Product Cross-Reference

ISM Element	MSS Product Used	Owner	Duration
Threat situation summary	INTSUM dashboard	35D / senior 35F	5–10 minutes
IPOE update (changes since last ISM)	IPOE workspace	35F (terrain); 35F (threat and COA)	5 minutes
I&W status update	I&W dashboard	35F / 35D	3 minutes

ISM Element	MSS Product Used	Owner	Duration
Collection coverage and gaps	CSM dashboard	35H	5 minutes
RFI status	RFI tracker	35H	3 minutes
Targeting update	Target status dashboard	35F (intel columns)	3 minutes
GEOINT update (new imagery or terrain changes)	GEOINT workspace	35G	As required
Coordination issues	As required	G2/S2 section chief	As needed
Production plan for next cycle	Production tracker	35D / section chief	3 minutes

F-3. ISM Output — Required MSS Actions After the Meeting

After each ISM, document the following in the appropriate MSS workspaces:

- PIR status updates: any PIR satisfied, expired, or transferred during the reporting period
- Collection gap actions: who is responsible for each gap resolution and by what deadline
- New requirements: new PIRs or IRs directed by the commander or S3 — enter in the collection management workspace
- IPOE updates directed at the ISM: assign to the responsible analyst with a completion suspense
- Targeting actions: new nominations, BDA follow-up requirements
- Product suspenses for the next ISM cycle

The section chief is responsible for ensuring ISM-directed MSS actions are completed within 24 hours.

APPENDIX G — INTELLIGENCE PRODUCT QUALITY STANDARDS

This appendix establishes minimum quality standards for intelligence products produced on MSS. These standards apply to all intelligence products briefed to or distributed to the commander.

G-1. Universal Product Quality Standards

Every intelligence product produced on MSS must meet these standards:

Standard 1: Classification marking. Products are marked with the correct overall classification based on derivative classification procedures (AR 380-5). Products that combine sources are assessed for combination classification. The classification appears prominently at the top of every product and at the top of every major section within it.

Standard 2: Data-as-of timestamp. The product displays when the data was last updated. Automated data elements display the system timestamp; analyst-entered assessments display the last-reviewed date. These are different and must appear separately.

Standard 3: Analyst attribution. The analyst who produced the assessment and the section chief who approved it are identified by name and position. Anonymous products are not authorized.

Standard 4: Confidence rating. Every significant analytical assessment carries an explicit confidence rating (High / Medium / Low) with a brief rationale statement. Products that present all assessments at the same confidence level — particularly all "High" — are flagged for re-review by the section chief.

Standard 5: Source citation. Key assessments cite the source category (HUMINT, GEOINT, SIGINT) and report reference. Products based on a single source say so explicitly. Products that appear to have multi-source support but trace to a single underlying report are corrected before distribution.

Standard 6: Analyst assessment text. Every intelligence product contains analyst-written assessment text — not just data visualization. The assessment addresses: current situation, key analytical finding, confidence level and basis, significant alternative, and intelligence gaps affecting the assessment.

G-1a. Characteristics of Effective Intelligence as Data Quality Criteria

FM 2-0 identifies seven characteristics of effective intelligence. These characteristics apply directly to MSS intelligence products and serve as data quality criteria for every product the intelligence section publishes.

Table G-0a. Seven Characteristics of Effective Intelligence — MSS Application (FM 2-0)

Characteristic	Definition	MSS Data Quality Application
Timely	Intelligence is available in time to support the commander's decision	Products display data-as-of timestamps; automated refresh intervals are set to support the battle rhythm; stale products are flagged and updated before briefing
Relevant / Tailored	Intelligence addresses the commander's specific requirements	Products are built against stated PIRs and CCIR; dashboards display only the indicators and data the supported commander requires — not everything the section collects
Accurate / Reliable	Intelligence correctly describes the situation	Source reliability and information credibility ratings (FM 2-22.3) are applied to all source data; confidence ratings accompany every analytical assessment; multi-source corroboration is documented
Predictive	Intelligence provides assessments of future conditions	Threat COA models include probability estimates; I&W dashboards track indicators tied to future threat actions, not just historical events
Usable	Intelligence is presented in a format the consumer	Products use standard formats (INTSUM, INTREP, SALUTE); dashboards are designed for the consumer's decision, not the

Characteristic	Definition	MSS Data Quality Application
	can act on	analyst's preference; export formats match the consumer's system
Complete	Intelligence provides sufficient detail for the decision at hand	Products identify known gaps explicitly; products that present partial information state what is missing and why; "no data" is displayed, not hidden
Precise	Intelligence provides the level of detail required	Location data uses MGRS to the appropriate precision; time data uses DTG format; quantitative assessments include ranges and confidence intervals where applicable

NOTE: These seven characteristics are not aspirational. They are the standard against which every intelligence product is evaluated. The section chief applies these criteria during product review (G-3). Products that fail to meet any characteristic are corrected before distribution.

G-2. Product-Specific Quality Standards

Table G-1. Product-Specific Quality Checklist

Product	Required Elements	Common Deficiencies to Check
INTSUM	Classification; period covered; threat summary; significant activity; collection summary; intelligence outlook; analyst text; data-as-of timestamp; analyst attribution; G2/S2 approval	Missing analyst assessment text; stale data presented without timestamp; all assessments rated "High confidence"
INTREP	Event description; location (MGRS); time; source reference; confidence rating; initial assessment	Missing confidence rating; event description without analyst assessment
SALUTE	All six elements: Size, Activity, Location (MGRS), Unit identification, Time, Equipment	Incomplete Location — missing MGRS; missing Equipment; missing Activity specificity
I&W Dashboard	All indicators with current status; last-updated timestamp; source reference for "Observed" indicators; COA linkage for each indicator	Indicators not updated since last ISM; "Observed" indicators without source citation
Threat Assessment	Threat capability by WFF; ORBAT summary; COA assessment; confidence ratings; key assumptions; key gaps	Capability assessment without confidence rating; COA assessment without probability estimate
GEOINT Product	Layer name (IAW Appendix A); collection date (not upload date); source; classification; exploitation annotations	Upload date used instead of collection date; exploitation annotations missing

G-3. Product Review Authority

Table G-2. Product Review and Approval Authority

Product	Primary Author	Reviewer	Approval Authority	Distribution Authority
INTSUM	35F / 35D	35D or 35X	G2/S2 section chief	G2/S2 section chief
INTREP (significant event)	35F	35D or 35X	G2/S2 section chief	G2/S2 section chief
SALUTE (routine)	Any analyst	35F or 35X	35X	Section standard
I&W Dashboard	35F / 35D	35D	G2/S2 section chief	G2/S2 section chief
Threat Assessment	35D	35X	G2/S2 section chief	G2/S2 section chief
GEOINT Product	35G	35D or 35X	G2/S2 section chief for targeting support	G2/S2 section chief
Target Package	35F / 35G	35D, targeting officer	G2/S2 section chief	Targeting officer
BDA	35G (physical) / 35D (functional/system)	35X	G2/S2 section chief	Targeting officer

CAUTION: Products distributed outside the intelligence section without G2/S2 section chief approval violate the chain of review and can result in uncorrected analytical errors reaching the commander. Urgency is not grounds for skipping the approval chain. The section chief must establish a streamlined approval process for time-sensitive products so that speed is achieved through process efficiency, not bypass.

APPENDIX H — INTELLIGENCE DOCTRINE CROSS-REFERENCE

This appendix cross-references the primary doctrinal publications governing intelligence operations in USAREUR-AF. MSS procedures in this manual are derived from — not substitutes for — these doctrinal references.

F-1. Primary Intelligence Doctrine References

Table F-1. Intelligence Doctrine Publications — MSS Relevance

Publication	Title	Relationship to MSS Use	Key Chapters
ADP 2-0	Intelligence	Foundation principles governing all intelligence functions; MSS operates within this framework	Chapters 1–3 (principles, functions, characteristics)
FM 2-0	Intelligence	Comprehensive reference for intelligence operations; defines intelligence cycle, all-source analysis, production standards	Chapters 2–4 (intelligence cycle, operations, technical tasks)
ATP 2-01	Planning Requirements and Assessing Collection	Collection management doctrine; PIR development, collection synchronization, RFI management	Chapters 2–4 (planning, collection, assessment)
ATP 2-01.3	Intelligence Preparation of the Battlefield	IPOE doctrine; all four steps, tools, and analytical products; MSS Chapter 2 is directly derived from this	All chapters
FM 2-22.3	Human Intelligence Collector Operations	HUMINT doctrine; source reliability standards, contact report procedures, collection management	Chapters 4–6 (collection, reporting, management); Appendix H (reliability ratings)
ATP 2-19.4	Brigade Combat Team Intelligence Officer	BCT S2 reference; integrates intelligence doctrine with BCT operational context	Chapters 2–5 (organization, operations, products)
FM 3-60	The Targeting Process	D3A methodology, target development, BDA; MSS Chapter 8 is derived from this	Chapters 2–5 (targeting process, nomination, execution, BDA)
AR 380-5	Army Information Security Program	Classification policy governing all MSS intelligence products	All
AR 381-10	U.S. Army Intelligence Activities	Legal framework for HUMINT and CI; MSS Chapter 6 compliance requirements	All
ATP 2-33.4	Intelligence Analysis	All-source analysis techniques, structured analytic techniques	All
ATP 2-22.9-1	PAI Research and Open-Source	Current OSINT/PAI research techniques; replaces inactive ATP 2-22.9	Chapters 3–4

Publication	Title	Relationship to MSS Use	Key Chapters
	Intelligence (Oct 2023)		
FM 3-55	Information Collection	Information collection planning, R&S integration	Chapters 2–3
FM 3-84	Intelligence Preparation of the Operational Environment (IPOE)	Theater-level IPOE procedures; complements ATP 2-01.3 at the operational and strategic echelon	All (supplements Chapter 2)
ADatP-36	Friendly Force Information (FFI)	NATO standard for real-time friendly force tracking data exchange — position reports, unit status	All
STANAG 5527	Friendly Force Tracking Systems Interoperability	NATO standard for BFT/FFT system interoperability across allied nations	All

Strategic Guidance:

The following are strategic guidance documents — not doctrine — that inform MSS training design and operational context.

Document	Authority	Relevance
NATO Digital Transformation Implementation Strategy (Oct 2024)	NATO	MDO interoperability context — frames intelligence data sharing in coalition operations
DDOF Playbook v2.2 (December 2025)	T2COM C2DAO	VAULTIS-A quality framework (8 dimensions); 6-phase data product lifecycle; 85% quality gate; MVP mandate 30 days

F-2. Doctrinal Alignment Checklist

Before conducting any intelligence function on MSS, confirm:

For IPOE (Chapter 2): - ☐ ATP 2-01.3 four-step framework is being applied (not just building geospatial layers) - ☐ IPOE products are designated as continuous process products with update triggers, not one-time deliverables - ☐ COA indicators are linked to specific NAIs and specific collection assets

For Collection Management (Chapter 3): - ☐ PIRs meet ATP 2-01 criteria: specific, answerable, timely, decision-linked - ☐ RFI tracking in MSS is supplementing (not replacing) formal RFI submission through the collection management system - ☐ Collection gaps are documented and briefed — not silently noted

For All-Source Analysis (Chapter 4): - ☐ Source reliability ratings are applied per FM 2-22.3, Appendix H - ☐ Information credibility ratings are applied per FM 2-22.3 standards - ☐ Analytical assessments include explicit confidence ratings with supporting rationale

For HUMINT and CI (Chapter 6): - ☐ AR 381-10 training is complete for all personnel with HUMINT/CI workspace access - ☐ No source identifying information in MSS — case numbers only - ☐ Privacy Act compliance verified with security manager for all screened-individual data

For Targeting Support (Chapter 8): - ☐ D3A methodology (FM 3-60) is the governing framework — not ad hoc targeting - ☐ Intelligence and fires sections have confirmed data ownership boundaries in the targeting workspace - ☐ BDA covers physical, functional, and system damage categories per FM 3-60

APPENDIX G — INTELLIGENCE SYNCHRONIZATION MEETING CHECKLIST

The ISM is the battle rhythm event where the G2/S2 presents the intelligence picture, reviews collection coverage, and coordinates intelligence requirements for the next cycle. MSS provides the data foundation for the ISM.

G-1. ISM Preparation Checklist (Complete Before the Meeting)

Intelligence Picture Verification: - ☐ INTSUM dashboard reviewed and assessment text is current (last reviewed within 24 hours) - ☐ All threat unit location objects have been reviewed for currency within 48 hours - ☐ COA indicator statuses confirmed against latest collection reporting - ☐ I&W dashboard status reviewed; any changes from last ISM documented - ☐ Pattern of life: any significant deviations from baseline in the last reporting period?

Collection Coverage Review: - ☐ Collection synchronization matrix reviewed: all PIRs and coverage status current - ☐ Collection gaps identified and documented: which PIRs have no current coverage? - ☐ RFI tracker reviewed: any overdue RFIs? Any new RFIs submitted since last ISM? - ☐ Collection reporting received: what new reporting has arrived since the last ISM? What PIRs does it satisfy or partially satisfy?

Production Status: - ☐ All scheduled products for this ISM are complete and available in MSS - ☐ Data-as-of timestamps verified for all dashboard products being briefed - ☐ Classification markings confirmed on all products being briefed

G-2. ISM Briefing Flow

ISM Element	MSS Product Used	Owner	Duration
Threat situation summary	INTSUM dashboard	35D / senior 35F	5–10 minutes
IPOE update	IPOE workspace review	35F (terrain/step 2); 35F (threat/step 3-4)	5 minutes
Collection coverage	CSM dashboard	35H	5 minutes
Collection gaps and RFIs	Gap panel; RFI tracker	35H	5 minutes
I&W status	I&W dashboard	35F / 35D	3 minutes
Targeting update	Target status panel	35F (intel columns)	3 minutes
Coordination issues	As required	G2/S2 section chief	As needed
Products for next cycle	Production tracker	35D	3 minutes

G-3. ISM Output — Required Actions

After each ISM, the following must be documented in the appropriate MSS workspace:

- PIR status updates (any PIR satisfied or expired during the reporting period)
- Collection gap actions (who is taking action on each gap, and by when)
- New requirements from the commander or S3 (enter as new PIRs or IRs)
- IPOE updates required based on the ISM discussion
- Targeting actions (new nominations, BDA follow-up requirements)
- Product suspenses for the next ISM cycle

APPENDIX H — BATTLEFIELD DAMAGE ASSESSMENT STANDARDS REFERENCE

BDA is the intelligence section's primary contribution to the post-strike phase of D3A. Quick reference standards for BDA completion in MSS.

H-1. BDA Categories and Standards

Physical Damage Assessment (PDA): Assesses the mechanical or structural damage to a target. PDA is primarily a 35G function, using post-strike imagery or observer reports.

Category	Definition	Required Evidence
PDA-1 Destroyed	Target is no longer functional and cannot be repaired	Direct imagery confirmation or multiple-source observer reporting
PDA-2 Severely Damaged	Target has received damage that prevents its immediate use	Imagery confirming major structural damage or observer reporting
PDA-3 Moderately Damaged	Target has received damage that limits its effectiveness	Imagery or reporting confirming partial structural damage
PDA-4 Lightly Damaged	Target has received minor damage with limited degradation	Imagery or reporting confirming minor structural damage
PDA-U Unknown	Damage level cannot be assessed from available collection	Document gaps; task additional collection

Functional Damage Assessment (FDA): Assesses whether the target can still perform its intended function. FDA is an all-source analyst function.

Category	Definition	Evidence Sources
FDA-A No function	Target cannot perform its military function	Observer reporting of no activity; imagery of abandoned/disabled equipment
FDA-B Severely degraded	Target can perform < 25% of normal function	Reduced activity reporting; imagery of partial capability remaining
FDA-C Moderately degraded	Target can perform 25–75% of normal function	Mixed reporting indicating partial capability
FDA-D Slightly degraded	Target can perform > 75% of normal function	Minimal indicators of degradation
FDA-U Unknown	Functional damage cannot be assessed	Document gaps; task collection against specific indicators

System Damage Assessment (SDA): Assesses degradation of the enemy's overall system or network capability resulting from the strike. SDA is a 35D / all-source function requiring multi-INT analysis.

System damage assessment requires: pre-strike baseline of the target's contribution to the system, post-strike collection showing changes in system behavior, and an analyst assessment of how the system compensated or failed to compensate for the loss.

H-2. BDA Entry Requirements in MSS

Table H-1. Required BDA Data Fields

Field	Content	Responsible	Required?
Strike date/time group	When the strike was executed	Fires section	Yes
Target object link	Link to the original HVT/HPT target object	Targeting officer	Yes
PDA category	Physical damage category (PDA-1 through PDA-U)	35G	Yes
PDA source	Source(s) supporting the PDA determination	35G	Yes
PDA date	Date the PDA was assessed (not the strike date)	35G	Yes
FDA category	Functional damage category	35D / 35F	Yes
FDA source	Sources supporting the FDA determination	35D / 35F	Yes
FDA date	Date the FDA was assessed	35D / 35F	Yes
SDA assessment	System/network damage narrative	35D	If applicable
Overall confidence	High / Medium / Low	35D / G2 section chief	Yes
Re-attack recommendation	Intelligence recommendation (not fires decision)	35D	Yes
BDA completion date	Date BDA entry was completed	35F	Yes

H-3. BDA Timeliness Standards

Phase	Standard	Responsible
Strike notification to intelligence	Within 1 hour of strike execution	Fires → Intelligence
BDA collection tasked	Within 2 hours of strike notification	35H
PDA initial entry (if imagery available)	Within 4 hours of imagery receipt	35G
FDA initial entry	Within 24 hours of first relevant reporting	35D / 35F
SDA entry	Within 48 hours of strike	35D

Phase	Standard	Responsible
Full BDA complete	Within 72 hours of strike, or earlier if re-attack decision pending	35D / G2 section chief

APPENDIX I — INTELLIGENCE SUPPORT TO THE MDMP

MSS provides the data environment for MDMP intelligence tasks. This appendix cross-references MDMP steps with the MSS products and workspaces supporting each step.

I-1. MDMP Intelligence Tasks by Step

Table I-1. MDMP Steps — Intelligence Tasks and MSS Products

MDMP Step	Intelligence Task	MSS Product / Workspace	Primary Owner
Step 1: Receipt of Mission	Review higher intelligence; update initial threat assessment	IPOE workspace — current INTSUM; threat model	35D / G2/S2
Step 2: Mission Analysis	Conduct IPOE Steps 1–4; brief IPB to commander	IPOE workspace (all four steps); COA indicator list	35F / 35D / 35G
Step 3: COA Development	Provide threat COAs; develop I&W indicators for each friendly COA	MLCOA/MDCOA overlays; indicator list	35D / 35F
Step 4: COA Analysis (War Game)	Conduct threat COA war game; develop decision support template	DST dashboard; COA overlay comparison	35D / 35F
Step 5: COA Comparison	Provide intelligence assessment of each friendly COA's risk	Threat assessment supporting COA comparison	35D
Step 6: COA Approval	Brief approved CCIR/PIR list to commander; finalize collection plan	PIR tracker; updated collection plan	G2/S2 / 35H
Step 7: Orders Production	Provide intelligence annex data; confirm CCIR list in MSS	CCIR-linked PIR objects; INTSUM for OPORD	G2/S2 / 35D

TASK BOX I-1: Prepare and Brief IPOE for MDMP Step 2 (Mission Analysis)

Conditions: Unit has received a new mission. G2/S2 has received the higher headquarters OPORD and intelligence annex. IPOE workspace has been established or updated for the new AOR. MSS access is operational. Time available for Mission Analysis brief preparation is defined by the unit's time management plan.

Standards: G2/S2 briefs all four IPOE steps to the commander and staff in a clear, logical sequence. All geospatial overlays are current, correctly named, and visible in MSS during the brief. COA overlays include both MLCOA and MDCOA with supporting indicators. The intelligence brief supports the commander's COA development — not just background awareness.

Procedure:

1. Review higher headquarters intelligence annex for the assigned mission. Load higher headquarters IPOE products into the unit IPOE workspace as received layers (separate from unit-produced layers; label with originating HQ).
2. Confirm AOR boundary layer is current and matches the assigned area in the OPORD. Update if the AOR has changed.
3. Update terrain trafficability layers for the new AOR. Coordinate with the engineer section for any specific obstacle data relevant to the new mission. Confirm weather data feed is current.
4. Update threat ORBAT for the new AOR: confirm all threat units in the AOR have current location objects, confidence ratings, and capability assessments.
5. Update COA overlays for the new mission context. MLCOA and MDCOA must reflect the new AOR terrain and the assigned friendly COA under development.
6. Develop indicator list for each COA. Link each indicator to a specific NAI and a collection asset. Confirm collection plan can cover all indicator NAIs.
7. Brief IPOE to the commander and staff:
8. Step 1: Define the OE — AOR boundaries, key actors, civil considerations. (3–5 minutes)
9. Step 2: Describe environmental effects — terrain analysis, key avenues of approach, weather impact. (5–8 minutes)
10. Step 3: Evaluate the threat — ORBAT, disposition, capability assessment, pattern of life. (5–8 minutes)
11. Step 4: Determine threat COAs — MLCOA and MDCOA with probability assessment, indicators, key intelligence gaps. (5–8 minutes)
12. After the brief, record all commander-directed intelligence requirements as new PIRs in the collection management workspace.

I-2. IPB Integration with MDMP Step 2

The G2/S2 brief during Mission Analysis covers all four IPOE steps and presents the commander with:

1. **Operational environment definition.** AOR boundaries, key terrain, adjacent unit positions, civil considerations.
2. **Environmental effects.** Terrain analysis — avenues of approach, key terrain, obstacles. Weather assessment — operational impact on visibility, mobility, and aviation.
3. **Threat evaluation.** Current ORBAT, threat disposition, capability assessment by WFF, pattern of life summary.
4. **Threat COAs.** MLCOA and MDCOA with supporting indicators. Probability assessment for each COA. Key intelligence gaps that could change the assessment.

All four steps must be briefable from MSS at the time of the Mission Analysis brief. The G2/S2 must confirm that the IPOE workspace is current before the brief — not during it.

I-3. Collection Plan Development During MDMP

The 35H builds the collection plan from PIRs developed during Mission Analysis and refines it as the MDMP produces the approved COA and CCIR list.

Collection plan MDMP timeline:

- Step 2 (Mission Analysis): Initial PIRs drafted; initial collection asset survey; initial NAI siting.
- Step 3 (COA Development): PIRs refined based on MLCOA/MDCOA indicators; NAIs positioned on terrain.
- Step 4 (COA Analysis): Collection plan stress-tested against the war game; gaps identified and addressed.
- Step 6 (COA Approval): Final CCIR/PIR list approved by commander; collection plan finalized in MSS.
- Between Steps 6 and 7: Collection plan briefed to collection assets; initial taskings issued.

I-4. The Intelligence Annex and MSS

The OPORD intelligence annex (Annex B) documents the intelligence picture, the threat assessment, and the PIR/CCIR framework for the operation. MSS products inform the Intelligence Annex but do not replace it. The Intelligence Annex is a classified document prepared in the authorized format.

When the OPORD is published, cross-check the Intelligence Annex against the MSS IPOE workspace to confirm:

- Threat ORBAT in the Annex matches the MSS threat model
- CCIR/PIR list in the Annex matches the PIR tracker in the collection management workspace
- NAIs in the Annex match the NAI objects in the IPOE workspace
- COA overlays in the Annex match the MSS COA overlay layers

Discrepancies between the Annex and MSS must be reconciled before the operation begins. The authoritative document is the signed OPORD; MSS must be updated to reflect it.

APPENDIX J — INTELLIGENCE PERSONNEL TRAINING STANDARDS FOR MSS

This appendix establishes minimum MSS training standards for intelligence personnel before assuming MSS duties at each proficiency level.

J-1. Intelligence MOS MSS Training Requirements

Table J-1. MSS Training Requirements by Intelligence MOS

MOS	SL 1 (Required)	SL 2 (Required)	SL 3 (Required)	SL 4A (Required)	Workspace Qualification	Verified By
35A (MI Officer)	Yes	Yes	Yes	Yes — full manual	All intelligence workspaces	35X or S2 section chief
35D (All-Source Officer)	Yes	Yes	Yes	Yes — full manual	All intelligence workspaces	G2/S2
35F (Intelligence Analyst)	Yes	Yes	Yes	Yes — Chapters 1, 2, 4, 7 minimum	Assigned workspaces	35X
35G (GEOINT Analyst)	Yes	Yes	Yes	Yes — Chapters 1, 5, 8 minimum	GEOINT workspace	35X or 35D
35H (Collection Manager)	Yes	Yes	Yes	Yes — Chapters 1, 3, 7 minimum	Collection management workspace	35X or G2/S2
35L (CI Agent)	Yes	Yes	Yes	Yes — Chapters 1, 6 minimum	CI workspace	G2/S2 (with security manager)
35M (HUMIN	Yes	Yes	Yes	Yes — Chapter 6 and safety	HUMINT workspace	G2/S2 (with HUMINT

MOS	SL 1 (Required)	SL 2 (Required)	SL 3 (Required)	SL 4A (Required)	Workspace Qualification	Verified By
T Collector)				summary minimum		Operations Cell)
35N (SIGINT Analyst)	Yes	Yes	Yes	Yes — Chapters 1, 4 minimum	SIGINT workspace (separate auth required)	G2/S2 and theater SIGINT authority
35T (MI Systems Maintainer)	Yes	Yes	Yes	Safety summary and Appendix E minimum	Admin access only	G6 and G2/S2
35X (Intel Senior Sergeant)	Yes	Yes	Yes	Yes — full manual	All intelligence workspaces	G2/S2

J-2. Workspace Qualification Standard

Before being granted write access to any intelligence workspace, the analyst must demonstrate:

1. Ability to navigate to the workspace without assistance
2. Ability to create the standard object types for that workspace with all required data fields
3. Ability to identify and apply the correct classification marking for the workspace
4. Understanding of the access control requirements for the workspace
5. Knowledge of the naming convention for objects within the workspace (Appendix A)
6. Understanding of the update cycle and update trigger requirements for the workspace

Qualification is verified by the 35X or G2/S2 through a direct observation check or written assessment, and is documented in the unit's training records.

J-3. Annual Recertification

All intelligence personnel with MSS workspace access complete annual recertification:

- Review of current version of SL 4A (verify no changes since initial qualification)
- Review of any workspace-specific updates or changes issued by the C2DAO
- Confirmation of security and classification handling standards

- Test of workspace proficiency for assigned workspaces

Recertification is documented in the unit's training management system and verified at each commander's inspection.

APPENDIX K — INTELLIGENCE INTEGRATION WITH OTHER WARFIGHTING FUNCTIONS

The Intelligence WFF supports all other WFFs. MSS enables this support through shared workspace access. This appendix identifies the primary intelligence products supporting each WFF and the workspace access coordination required.

K-1. Intelligence Support to Fires

Intelligence is the most tightly coupled WFF with Fires in the targeting cycle. See Chapter 8 for detailed targeting integration procedures. Summary of MSS integration points:

- Targeting workspace: shared write access (intelligence columns); fires section has read access to all intelligence products
- HVT/HPT tracker: intelligence updates location and confidence; fires plans attack
- BDA: intelligence provides physical/functional/system assessment; fires provides effects summary and re-attack recommendation
- IPOE COA overlays: fires references threat COA overlays to plan fire missions; fires does not edit intelligence IPOE products

Table K-1. Intelligence-Fires MSS Integration Summary

MSS Product	Intelligence Provides	Fires Receives	Update Standard
HVT/HPT tracker	Location, confidence, target analysis	Read access	Within 2 hours of new locating report
TSM	Collection column, intelligence assessment column	Read; write attack column	At each targeting board
COA overlays	MLCOA/MDCOA with indicators	Read access for fire planning	At each IPOE update
BDA	Physical/functional/system assessment	Read; adds effects/re-attack recommendation	IAW Appendix H standards

K-2. Intelligence Support to Movement and Maneuver

Intelligence provides maneuver commanders with the threat picture supporting scheme of maneuver development and execution. MSS products shared with maneuver elements:

- INTSUM dashboard: read access for all maneuver battalion and brigade commanders
- IPOE terrain overlays: terrain trafficability and key terrain available for maneuver planning
- Threat ORBAT: current threat disposition available to maneuver commanders (read access, not write)
- I&W dashboard: read access for the S3 and maneuver commanders to monitor threat COA indicators

Access for maneuver elements is read-only. Maneuver commanders do not edit intelligence products. Coordinate with the S3 to determine what level of IPOE product detail is appropriate for maneuver section access.

K-3. Intelligence Support to Sustainment

Intelligence support to sustainment focuses on threat to the MSR/ASR network, route security requirements, and CSS facility protection. MSS products supporting sustainment:

- Threat activity overlays showing activity along MSRs/ASRs
- Pattern of life data on threat activity patterns affecting sustainment routes
- Indicator tracking for threat interdiction of sustainment routes

Sustainment access to intelligence MSS products is limited to: threat activity data relevant to MSR/ASR corridors, pattern of life summaries for route security planning. Full IPOE and threat assessment products are not provided to sustainment sections without G2/S2 review and approval.

K-4. Intelligence Support to Mission Command

The intelligence section provides the S3 with the intelligence picture supporting the operations process. MSS integration with the Mission Command workspace (SL 4F):

- CCIR dashboard: PIR-derived CCIR components appear on the S3's unified CCIR dashboard (coordinate with S3 for data sharing)
- INTSUM: available for access by the S3 and XO (read-only)
- Threat COA overlays: available in the common operating picture layer for S3 review

Coordinate with the S3 at the beginning of each operational period to confirm which intelligence products will appear on the Mission Command workspace and what access level is authorized.

K-5. Intelligence Support to Protection

CI and force protection intelligence is the bridge between the Intelligence WFF and the Protection WFF. MSS CI products supporting protection:

- CI indicator tracking: hostile intelligence activities, surveillance detection, penetration indicators
- Personnel security: CI screening data (non-identifying) supporting access control recommendations
- Physical security: threat activity data supporting base defense planning

Protection elements receive read access to CI-derived indicator data that is relevant to force protection — not access to the CI workspace itself. The 35L coordinates directly with the S2 and the unit Provost Marshal to determine appropriate sharing.

K-6. Intelligence Integration with Civil Affairs

Civil considerations in IPOE are developed in coordination with the Civil Affairs team. MSS civil considerations layers are built with CA team input and validated against CA assessments. CA teams may receive read access to the civil considerations layer of the IPOE workspace — with G2/S2 approval — to review the intelligence assessment of civil factors affecting their operations.

The intelligence section does not own the civil information gathered by CA during operations. CA-gathered civil information feeds the IPOE civil considerations layer through a defined contribution process, not through direct CA write access to intelligence workspaces.

APPENDIX L — INTELLIGENCE SECTION BATTLE RHYTHM MANAGEMENT

The intelligence section battle rhythm defines when specific MSS products are produced, updated, and briefed. This appendix provides a standard battle rhythm template that units adapt to their operational tempo.

L-1. Standard Daily Intelligence Battle Rhythm Events

Table L-1. Standard Daily Intelligence Battle Rhythm — MSS Products

Time	Event	MSS Product Required	Owner	Preparation Lead Time
0600	Morning intelligence update	INTSUM dashboard current; I&W status current	35F / 35D	1 hour
0700	Battle Update Assessment (BUA)	INTSUM; threat model; CCIR status; any significant I&W changes	G2/S2	Confirm 30 min before

Time	Event	MSS Product Required	Owner	Preparation Lead Time
1000	Intelligence Synchronization Meeting	Full ISM package (Appendix F)	Section chief	1 hour
1400	Targeting board	TSM current; target status dashboard; BDA updates	35F / 35G	30 minutes
1700	Evening intelligence update	INTSUM updated for PM cycle; any I&W changes; SIGACT summary	35F	30 minutes
2200	Night shift update	I&W dashboard confirmed current; any significant activity entered	On-call analyst	Continuous

L-2. Battle Rhythm Management in MSS

The intelligence section manages battle rhythm product delivery through the production tracker in the all-source analysis workspace. The production tracker displays: all products, their delivery times, assigned analyst, and current status (Pending / In Progress / Complete / Briefed).

Production tracker management. The 35D or section chief reviews the production tracker at the start of each shift. Any product that is "Pending" but not in progress two hours before its delivery time is flagged for immediate action. Products that are "Complete" but not yet confirmed "Briefed" are followed up with the consumer.

L-3. Battle Rhythm Adjustment During Operations

The standard battle rhythm is the peacetime or steady-state template. During active operations or periods of high analytical activity, the section chief adjusts the battle rhythm:

- Increase INTSUM frequency from daily to every 12 hours or every 8 hours as required
- Add interim I&W updates when indicator activity is high
- Accelerate targeting board cadence when the targeting cycle is active
- Add dedicated SIGACT analysis update when collection reporting volume is high

Any battle rhythm change requires G2/S2 approval and coordination with the S3 to ensure intelligence products continue to support the operations process timing.

TASK BOX L-1: Establish Intelligence Section Battle Rhythm on MSS

Conditions: Unit is preparing for an operational period or exercise. The operations section (S3) has established the unit battle rhythm. G2/S2 has received the battle rhythm schedule. MSS workspaces are established and operational.

Standards: All intelligence section battle rhythm events are entered in the production tracker. Product suspenses, assigned analysts, and MSS products required for each event are documented. G2/S2 has reviewed and approved the production plan. S3 has confirmed intelligence products will be available at the required times for each battle rhythm event.

Procedure:

1. Obtain the unit battle rhythm schedule from the S3. Identify all battle rhythm events that require intelligence products or G2/S2 attendance.
2. For each battle rhythm event requiring intelligence input, identify: the MSS product(s) required, who produces them, when they must be complete (work backward from the event time), and how they are delivered (briefed in person; available on MSS for review; exported and distributed).
3. Enter each production task in the production tracker in the all-source analysis workspace: event name, product required, assigned analyst, completion suspense, delivery method.
4. Brief the production plan to the section. Confirm each analyst understands their production tasks, suspense times, and MSS workspace procedures.
5. Coordinate with the S3 to confirm which intelligence products will appear on the Mission Command workspace CCIR dashboard (SL 4F coordination).
6. Review the production plan after the first battle rhythm cycle. Adjust suspense times based on actual production experience.

APPENDIX F — RELATED MANUALS AND TRAINING TRACKS

WFF Peer Tracks

SL 4A is one of six Warfighting Function tracks at the same tier. All six WFF tracks require SL 1, SL 2, and SL 3 as prerequisites. Intelligence practitioners should develop working familiarity with SL 4B (Fires) and SL 4F (Mission Command) — the two WFF tracks with the most intensive intelligence data coordination requirements.

Table F-1. WFF Peer Track Quick Reference

Track	Title	Prerequisite	Primary Intel Coordination Point
SL 4A	Intelligence WFF	SL 1 + SL 2 + SL 3	This manual
SL 4B	Fires WFF	SL 1 + SL 2 + SL 3	Targeting workspace, AMD coordination

Track	Title	Prerequisite	Primary Intel Coordination Point
SL 4C	Movement and Maneuver WFF	SL 1 + SL 2 + SL 3	NAI/TAI overlays, reconnaissance reporting
SL 4D	Sustainment WFF	SL 1 + SL 2 + SL 3	LOC threat data, supply point security
SL 4E	Protection WFF	SL 1 + SL 2 + SL 3	AT intelligence integration
SL 4F	Mission Command WFF	SL 1 + SL 2 + SL 3	PIR-derived CCIR, INTSUM dissemination

Specialist Tracks (Prerequisite: SL 3)

For technical specialists pursuing advanced analytical or engineering capability, specialist tracks are available after completing SL 3 (Advanced Builder). These are not required for intelligence WFF employment.

Table F-2. Specialist and Advanced Track Quick Reference

Track	Title	Advanced Track
SL 4G	ORSA	SL 5G
SL 4H	AI Engineer	SL 5H
SL 4M	ML Engineer	SL 5M
SL 4J	Program Manager	SL 5J
SL 4K	Knowledge Manager	SL 5K
SL 4L	Software Engineer	SL 5L

APPENDIX M — PROFESSIONAL READING LIST

Curated articles from Army professional journals and military publications. These supplement doctrinal references with contemporary operational perspectives.

Source	Title	Date	Relevance
MIPB	"FRIDAY: Unlocking OSINT for a Data-Driven Army"	2025	OSINT and data-driven intelligence
MIPB	"Intelligence Support to Information Advantage"	Jan-Jun 2026	Intel support to info advantage
MIPB	"Army Transitioning to Support Deep Sensing in MDO"	Jul-Dec 2025	Deep sensing and multi-domain intel

Source	Title	Date	Relevance
MIPB	"Open-Source Intelligence Support to Targeting"	2024	OSINT-to-targeting pipeline
Military Review	"Exploring AI-Enhanced Cyber and Information Ops"	Mar-Apr 2025	AI in cyber/info ops

---

This publication supersedes all previous SL 4A drafts.

Review date: 18 months from version date. Next review: September 2027.

DoD and Army Strategic References:

- **JADC2 Strategy Summary (March 2022)** — Cross-domain data integration strategy for Joint All-Domain Command and Control
- **DoD Directive 3000.09, Autonomy in Weapon Systems (January 2023 update)** — Policy on autonomous and semi-autonomous functions in weapon systems; context for AI-enabled intelligence systems
- **DDOF Playbook v2.2 (December 2025)** — T2COM C2DAO; VAULTIS-A quality framework (8 dimensions); 6-phase data product lifecycle; 85% quality gate; MVP mandate 30 days