CONCEPTS GUIDE

SL 4A

USAREUR-AF

CONCEPTS GUIDE — SL 4A COMPANION — INTELLIGENCE WARFIGHTING FUNCTION · 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

CONCEPTS GUIDE — SL 4A COMPANION — INTELLIGENCE WARFIGHTING FUNCTION · MAVEN SMART SYSTEM (MSS)

Forward: Intelligence has always been a data discipline. What MSS changes is the speed of integration and the visibility of gaps — not the analytical process itself. Intelligence practitioners who understand this distinction will use the platform effectively. Those who do not will either underuse it (treating it as just another database) or overuse it (letting the platform substitute for analytical judgment). **Prereqs:** SL 1 (Maven User), SL 2 (Builder), and SL 3 (Advanced Builder). This guide assumes platform familiarity and focuses on conceptual integration — how intelligence doctrine, tradecraft, and the MSS data environment relate to each other. SL 3 is required before beginning SL 4A; read this Concepts Guide after SL 3 and before beginning the SL 4A task manual. **Purpose:** This guide is a conceptual companion to SL 4A. It develops the mental models that intelligence practitioners need before operating MSS in an intelligence role. Read this guide before beginning SL 4A. It contains no step-by-step procedures — those are in the TM. This guide develops understanding. The TM develops skill. *HQ USAREUR-AF · v1.0 · 2026 · DISTRIB: USG only*

SECTION 1 — INTELLIGENCE AND DATA: THE INTEL PRACTITIONER'S MENTAL MODEL

BLUF: Intelligence has always been a data discipline. What MSS changes is the speed of integration and the visibility of gaps — not the analytical process itself. Intelligence practitioners who understand this distinction will use the platform effectively. Those who do not will either underuse it (treating it as just another database) or overuse it (letting the platform substitute for analytical judgment).

Intelligence Is Information Plus Analysis

ADP 2-0 defines intelligence as the information and knowledge about the enemy, weather, and terrain necessary to support decisionmaking (ADP 2-0, para 1-2). The word "knowledge" is load-bearing. Data is not intelligence. A SIGACT entry is not intelligence. A collection of SALUTE reports is not intelligence. Intelligence is what a trained analyst produces when they apply judgment, doctrine, and tradecraft to data collected about a specific enemy, in a specific environment, for a specific commander's decision.

MSS is a data platform. It collects, normalizes, integrates, and visualizes data. It does not assess. It does not evaluate source reliability. It does not determine whether an observed enemy activity is a feint or the main effort. These are analytical functions performed by human intelligence professionals.

The mental model: MSS is the library. The analyst is the scholar. A larger, better-organized library does not make a mediocre scholar into a great one — but it does allow a great scholar to work faster, see more, and miss less.

NOTE: ADP 2-0 identifies four principles of intelligence: synchronization, integration, agility, and continuity (ADP 2-0, para 1-8). All four are data-dependent. MSS improves the data foundation for all four principles simultaneously. This is its core operational value.

What Changes With MSS — and What Does Not

What changes: - Data assembly time. Before MSS, analysts spent a significant portion of their time aggregating data from disparate sources — DCGS-A, unit reporting, email, slide products. MSS integrates these feeds, returning that time to analysis. - Visibility of gaps. On MSS, a PIR with no collection coverage is visible to everyone in the intelligence section simultaneously, without a separate meeting to surface it. Collection gaps are harder to miss. - Product accessibility. An INTSUM published in MSS is immediately available to every credentialed user at every echelon — no separate distribution required. - Pattern analysis. Manually detecting temporal or geographic patterns in SIGACT data required significant analyst effort. MSS tools surface patterns faster and allow analysts to spend more time interpreting them.

What does not change: - The intelligence process. Plan and direct, collect, process, produce, disseminate. MSS supports each phase; it does not replace any of them (FM 2-0, para 2-1). - Source evaluation. The reliability of a source is a human judgment based on track record, access, motivation, and corroboration. MSS can display source reliability ratings; it cannot determine them. - Analytical confidence. An analyst's confidence in an assessment derives from the quality and quantity of corroborating evidence and the quality of the analytical reasoning applied. MSS does not generate confidence — it provides data from which confidence is built. - Analytical authority. The S2 is responsible for the intelligence picture. MSS does not diffuse that responsibility. The section chief who approves a flawed INTSUM is responsible for the flawed product, whether or not MSS generated the underlying data.

The Intelligence Practitioner's MSS Operating Assumption

Every intelligence practitioner using MSS should internalize one operating assumption before beginning work:

MSS shows what has been reported. Not what has happened. Not what the enemy is doing. What has been reported.

Reported data is filtered through reporting chain latency, source access, collection coverage gaps, and normalization error. The gap between the ground truth and the reported picture is the analytical problem that intelligence professionals exist to solve. MSS narrows that gap — it does not close it.

SECTION 2 — THE INTELLIGENCE PROCESS AND MSS: WHERE THE PLATFORM FITS

BLUF: MSS is not a replacement for the intelligence process — it is a data layer within it. Each phase of the intelligence process (FM 2-0) maps to specific MSS capabilities. Understanding where MSS adds value in each phase prevents both underuse and analytical over-reliance.

Mapping the Intelligence Process to MSS

Table 2-1. Intelligence Process Phase to MSS Capability

Phase	Doctrinal Purpose	MSS Adds	MSS Does Not Add
Plan and Direct	Determine requirements; develop collection plan; direct collection	PIR tracking; CSM visualization; collection gap alerting; RFI lifecycle management	Analytical judgment about what to collect; assessment of collection feasibility
Collect	Execute collection tasks; report results	Collection status monitoring; feed integration from DCGS-A and other sources; HUMINT report ingestion	Collection execution (MSS does not collect); source access
Process	Convert information to usable form; source evaluation	Data normalization; geolocation; time-stamping; duplicate detection	Source reliability determination; credibility assessment; translation
Produce	Analysis; intelligence product creation	Integrated data environment; visualization tools; product workspace; INTSUM/SIGACT tools	Analysis; assessment; analytical confidence; finished intelligence
Disseminate	Timely conveyance to users	Immediate multi-echelon product access; push notification; product archive	Ensuring intelligence reaches the right decision-maker at the right time (still a human coordination function)

The "Analysis Gap" — Where MSS Ends and Tradecraft Begins

The most important column in Table 2-1 is "MSS Does Not Add" for the Produce phase: analysis, assessment, analytical confidence, finished intelligence. These are the core functions of the intelligence section. They happen in the analyst's mind, informed by training, experience, and doctrine — not in a platform.

MSS can show you that enemy activity in a specific grid square has increased 40 percent over the last seven days. It cannot tell you why, what it means, or what the commander should do about it. The analyst determines whether this is an indicator of offensive preparation, a deception operation, logistics reconstitution, or an anomaly in reporting. That determination requires knowledge of OPFOR doctrine, understanding of the specific threat's historical behavior, evaluation of collection source quality, and synthesis with other indicators from other INT disciplines.

NOTE: FM 2-0 describes intelligence production as "analysis and conversion of processed information into intelligence" (FM 2-0, para 2-21). The word "conversion" implies transformation — not just display. MSS displays. Analysts convert. Both are required; only one is a human function.

The Production Cycle and MSS Rhythm

The intelligence production cycle — the recurring loop of collection reporting, processing, analysis, and product delivery — must be synchronized with the battle rhythm. MSS supports this synchronization through the intelligence synchronization matrix, which maps collection windows and product suspenses against battle rhythm events.

The mental model for production cycle management: every intelligence product on MSS should have a clear answer to three questions: Who produces it? When is it due? Which battle rhythm event does it support? Products without clear answers to these three questions accumulate in MSS workspaces without ever reaching the commander.

SECTION 3 — IPB MENTAL MODEL: THINKING WITH INTEGRATED DATA

BLUF: IPB is the analytical framework that structures the intelligence section's understanding of the operational environment and the threat. MSS does not change the IPB framework — it changes the data inputs available for each step. The mental model shift required: IPB is no longer constrained by data availability in the same way it was in a manual environment. The constraint is now analytical bandwidth, not data.

IPB as a Living Process, Not a One-Time Product

ATP 2-01.3 defines IPB as "a systematic, continuous process" (ATP 2-01.3, para 1-1). The word "continuous" is often lost in practice. IPB products are produced during planning and then frequently treated as static artifacts. With MSS, the data environment enables continuous IPB — products can and should be updated as collection provides new information about terrain changes, threat repositioning, or environmental conditions.

The mental model: think of each IPB product on MSS as a living document with a defined update trigger, not a deliverable submitted once and filed. The MCOO should have an update trigger (bridge status change, new collection on obstacle). The event template should have an update trigger (collection confirms or denies COA indicator). The DST should have update triggers (decision points reached or invalidated).

NOTE: ATP 2-01.3 specifies that IPB supports "the entire operations process" (ATP 2-01.3, para 1-4). This means IPB is not complete when the OPORD is published — it continues through execution and assessment. MSS enables this continuity by maintaining IPB products as data objects that update on new collection, not as PowerPoint slides that are re-briefed from scratch.

The Terrain-Threat-Collection Triangle

The conceptual heart of IPB is the relationship among three analytical domains:

1. **Terrain and environment** (Steps 1-2): What does the physical environment permit, restrict, and channel?
2. **Threat** (Step 3): How does the enemy operate, and how does the environment affect enemy options?
3. **Collection** (Steps 3-4, flowing into collection management): What can we observe, and where?

MSS integrates data for all three domains in a single geospatial environment. This integration is the platform's most significant contribution to IPB. Before MSS, an analyst building an event template had to mentally reconcile terrain analysis from one product, OPFOR doctrinal templates from a separate database, and collection asset positions from a third source. On MSS, these layers can be overlaid on a single geospatial display.

The integration reveals relationships that were hard to see manually. A mobility corridor that appears attractive for an OPFOR avenue of approach may be covered by an existing ISR asset — or uncovered, revealing a collection gap that would leave the decision support template unsupported. MSS makes this relationship visible immediately.

The MCOO as the Foundation Layer

Of all IPB products, the MCOO is the most foundational for MSS use because it is the base geospatial layer on which all subsequent products are built. The MCOO quality directly determines the analytical quality of avenues of approach analysis, event template placement, and NAI siting.

A low-quality MCOO — missing bridge data, outdated obstacle information, imprecise mobility corridor boundaries — propagates analytical error through every subsequent IPB product built on top of it. Intelligence sections should invest analytical effort in the MCOO proportional to its role as the foundational layer.

NOTE: The 35G analyst who owns the MCOO on MSS should maintain a change log — documenting what changed, when, and based on what reporting. This creates an analytical audit trail and supports historical analysis when the question arises: "What did we know about this terrain corridor, and when did we know it?"

SECTION 4 — COLLECTION MANAGEMENT MENTAL MODEL: PIR, RFI, AND THE LIMITS OF MSS

BLUF: Collection management is the mechanism that connects the commander's intelligence requirements to the collection assets that answer them. MSS makes this connection visible and trackable. The mental model shift: collection management on MSS is a data discipline, and data discipline failures produce intelligence failures even when collection assets are fully operational.

PIR as an Analytical Specification

A PIR is not just a question on a list. A PIR is an analytical specification — it defines what the intelligence section needs to know, why it matters (which decision it supports), when it must be answered, and what observable indicators would constitute an answer. A PIR that is vague, incorrectly scoped, or disconnected from a specific commander's decision is not a PIR — it is a wish.

The quality of PIR development determines the quality of the collection plan. A collection plan built on poor PIRs will produce data that is technically collected but analytically useless — data that does not answer the commander's questions because the questions were never properly defined.

MSS makes PIR quality more visible than it was in a manual environment. A PIR without defined triggering indicators cannot be monitored on MSS. A PIR without an assigned collection asset will generate a persistent gap indicator. Poor PIR quality shows up as collection management dysfunction on MSS, which surfaces it for correction.

NOTE: ATP 2-01 requires that PIRs be specific, answerable, timely, and decision-linked (ATP 2-01, para 2-3). These criteria are unchanged by MSS. MSS simply makes non-compliant PIRs more visible — a collection gap on the dashboard often traces back to a PIR that was too vague to task against.

The RFI as a Collection Gap Formalized

An RFI is a collection gap that organic assets cannot fill. The RFI process formalizes that gap and routes it to higher, where different collection assets may be available. On MSS, the RFI tracker makes the collection gap visible to the entire intelligence section and provides accountability for gap closure.

The mental model: every open RFI is an unresolved intelligence question that is degrading the quality of the intelligence picture. RFI management is not administrative work — it is analytical work that directly affects the commander's information environment. An RFI that disappears into the tracking system and is never followed up is a collection gap that the commander does not know exists.

The Limits of MSS in Collection Management

MSS cannot task collection assets. This is the most important limitation to understand. The collection synchronization matrix on MSS shows what assets are tasked and what PIRs they cover. It does not issue the task. Formal collection tasking goes through the appropriate collection management system (DCGS-A, CPCE, or service-specific systems). MSS integrates the picture; it does not replace the tasking mechanism.

Similarly, MSS cannot compel collection reporting. An asset assigned on the CSM but not reporting is a real-world failure — a crew that did not execute, a system that did not transmit, or a pipeline that did not ingest. MSS makes the non-reporting visible; it does not fix the underlying problem.

Table 4-1. What MSS Can and Cannot Do in Collection Management

Function	MSS Can	MSS Cannot
PIR management	Track, display, and monitor PIRs	Develop PIRs; assess PIR quality
Collection asset assignment	Display assignments; flag gaps	Task assets; issue collection orders
RFI lifecycle	Track lifecycle from submission to closure	Submit RFIs through formal channels; compel higher to respond
Gap analysis	Automatically surface PIRs with no coverage	Fill gaps; substitute for missing collection
Collection reporting	Ingest and display incoming reports	Collect; execute sensor operations

SECTION 5 — THE ALL-SOURCE FUSION CHALLENGE: WHY MSS DOES NOT ANALYZE

BLUF: All-source fusion is the analytical process of integrating information from multiple intelligence disciplines to produce a more complete and reliable intelligence picture than any single source can provide. MSS enables all-source fusion by co-locating multi-source data. It does not perform fusion. Understanding this distinction prevents the most dangerous failure mode in intelligence operations on MSS: treating integrated data as finished intelligence.

What All-Source Fusion Actually Is

FM 2-0 describes all-source intelligence as intelligence derived from multiple sources and intelligence disciplines (FM 2-0, para 3-5). The analytical process that produces all-source intelligence involves:

1. **Corroboration.** Does information from one source confirm, contradict, or add detail to information from another source? Corroborated information is more reliable than single-source reporting.
2. **Source deconfliction.** Are two reports describing the same event, or two different events? Single-source reports that appear to confirm each other may both trace to the same original observation — not independent confirmation.
3. **Pattern recognition.** Across multiple sources and time, what patterns emerge? A single SIGACT may be insignificant. A pattern of SIGACTs may indicate operational preparation.
4. **Gap identification.** What is NOT being reported that should be, given the OPFOR's doctrine and the current situation? Absence of reporting in a key NAI may be more significant than the presence of reporting.
5. **Assessment.** Given all available information, what is the most likely explanation? What is the commander's risk if the most dangerous alternative is true?

MSS co-locates the data for steps 1 through 4 in a common environment. The analyst performs all five steps using judgment, tradecraft, and doctrine. Step 5 — assessment — is entirely human.

The Integration Trap

When multiple data sources produce consistent information in MSS — SIGINT indicating enemy movement, HUMINT confirming enemy activity, SIGACT data showing increased enemy contact in the same area — the integrated picture can appear to "speak for itself." This is the integration trap: the analyst mistakes data consistency for analytical certainty.

Consistent data from multiple sources is valuable. But it is not automatically accurate. Enemy deception operations are specifically designed to produce consistent, misleading indicators across multiple collection disciplines. An analyst who trusts the integration trap rather than applying critical analytical

judgment will fail against a sophisticated adversary.

The antidote to the integration trap is analytical discipline: explicitly stating confidence levels, explicitly identifying alternative explanations, and explicitly documenting the reasoning behind the assessment — not just the data that supports it.

NOTE: FM 2-0 structured analytic techniques (SATs) — including alternative analysis, red teaming, and devil's advocacy — exist precisely to counter the integration trap (FM 2-0, para 2-26). MSS does not replace the need for SATs. In fact, an integrated data environment that makes consistent patterns more visible may increase the need for disciplined alternative analysis.

What the 35D Does That MSS Cannot

The 35D (All-Source Intelligence Officer) is the human analyst responsible for the all-source fusion process. The 35D's analytical functions — which MSS cannot replicate — include:

- Evaluating source reliability based on historical performance, access, and motivation
- Determining whether reporting from different sources is independently corroborated or traces to a single original observation
- Applying OPFOR doctrinal knowledge to evaluate whether observed behavior is consistent with the threat's doctrine
- Constructing and evaluating alternative explanations for the observed data
- Making a confidence-weighted analytical judgment and defending it to the commander
- Identifying what the data does NOT show that the enemy's most dangerous COA would require

The value of the 35D to the commander is not the ability to retrieve integrated data from MSS — any trained platform user can do that. The value is the analytical judgment applied to that data.

SECTION 6 — SECURITY AND HANDLING MENTAL MODEL: CLASSIFICATION IN AN INTEGRATED ENVIRONMENT

BLUF: MSS is an integrated environment, which means classification errors have integrated consequences. A mishandled SIGINT product in a siloed system stays in that system. A mishandled SIGINT product in MSS may appear in shared workspaces, COP layers, and dissemination products before the error is caught. Classification discipline on MSS is not just personal compliance — it is a force protection function.

Classification Inheritance

When a data product is published in MSS, it inherits the classification requirements of its most sensitive source component. An INTSUM that incorporates declassified SIGINT, non-attributable HUMINT, and GEOINT products carries the classification of the highest-classification source it incorporates. Classification marking in MSS is not automated — it is the analyst's and section chief's responsibility to apply the correct marking.

This requires analysts to understand the classification level of every source that contributed to a product. In the rush of a production cycle, this step is frequently abbreviated or skipped. The result is products with incorrect classification markings — usually under-classified, which creates a security risk, but occasionally over-classified, which creates an unnecessary access problem.

NOTE: AR 380-5 governs classification and security of information. Applicable SIGINT security directives govern SIGINT classification. Intelligence practitioners on MSS are responsible for knowing the applicable security rules for their assigned INT disciplines, not just general classification policy.

The OPSEC Dimension of Collection Management Data

Collection management data — the PIR list, the collection synchronization matrix, the gap analysis — reveals the intelligence section's requirements, capabilities, and vulnerabilities. A hostile intelligence service that obtained access to the unit's PIR list would know precisely what the unit does and does not know about enemy activity, and could use that information to design deception operations or protect activities the unit is not tracking.

This means collection management data requires OPSEC handling, not just classification handling. Collection management products should not be printed and left unattended, discussed in unsecured communications, or shared with personnel who do not have a need to know — even if they have the appropriate clearance.

MSS workspaces for collection management should have access permissions that match need-to-know, not just clearance level. Coordinate with the S6 on workspace access control configuration.

The HUMINT Source Protection Imperative

HUMINT source protection is the highest-stakes security discipline in intelligence operations. The exposure of a human source can result in the death of that source, the compromise of the collection network, and long-term damage to the unit's intelligence capabilities. Source identity is classified at the highest levels, and the restriction is absolute — source identity belongs in designated classified HUMINT source management systems, not in MSS.

This is not a procedural nuance. It is a fundamental principle of HUMINT tradecraft. Every 35M and every 35F who handles HUMINT reporting on MSS must internalize this principle before they touch any HUMINT data.

The practical implication: HUMINT reports on MSS contain the intelligence information derived from collection, not the collection methodology, not the source description, and never the source identity. If a report on MSS contains any field that could identify a source, that entry must be corrected immediately and the matter reported to the section chief and the HUMINT Operations Cell.

NOTE: FM 2-22.3 states that "source identity is classified at a level that prevents unauthorized access" (FM 2-22.3, para 5-2). This level is typically higher than the classification of the intelligence reporting itself. The two must be handled separately, always.

Cross-Domain Considerations

MSS operates within a defined classification domain. Some intelligence data exists at higher classification levels that may not flow into the standard MSS environment. Intelligence practitioners must understand:

- What intelligence data is available at the MSS classification level
- What data exists at higher levels and is not available in MSS
- When a product requires higher-classification source data and therefore cannot be fully produced in MSS
- Who approves cross-domain data transfers when portions of a product must move between classification levels

Coordinate with the S6 and the unit IMO for specific cross-domain procedures at your echelon. Do not assume a product is complete because MSS data is integrated — consider whether the product is missing relevant higher-classification data that would change the assessment.

SECTION 7 — COMMON FAILURE MODES FOR INTELLIGENCE PRACTITIONERS ON MSS

BLUF: MSS failure modes for intelligence practitioners are distinct from those of other WFF users. Intelligence failures on MSS tend to involve analytical over-reliance on integrated data, collection management data discipline failures, and security errors unique to the intelligence data environment. This section describes the most common failure modes, with root cause analysis and correction.

Failure Mode 1: Treating Integrated Data as Finished Intelligence

Description. The analyst publishes an INTSUM or briefs a commander product that recites data from MSS without applying analytical judgment. The product describes what the data shows without assessing what it means, why it matters, or what the commander should consider.

Cause. Time pressure. The integrated data environment in MSS makes it easy to assemble a product quickly. When the production clock is running, the temptation to move from "data assembled" to "product published" without the analytical step is significant.

Why it fails. Data is not intelligence. A commander who receives a product listing SIGACTs without an assessment is receiving raw data, not intelligence support. The intelligence section's function is analysis, not data delivery. An S2 who only aggregates data is performing a data technician function, not an intelligence officer function.

Correction. Every intelligence product on MSS must contain an explicit assessment section — not just a data summary. The assessment must: state the most likely enemy COA; identify the key indicators supporting that assessment; acknowledge the most dangerous alternative; and state the analyst's confidence level and its basis. If there is no time to write the assessment, there is no time to publish the product.

Failure Mode 2: PIR List Decoupled from Commander's Decisions

Description. The PIR list in MSS is populated at the beginning of an operation and is not updated as the commander's decisions and the situation evolve. PIRs that are no longer relevant remain active; new intelligence requirements arising from operational developments are not added.

Cause. The PIR list feels like a planning product — something produced during MDMP and then maintained as a reference. In practice, the commander's decisions and decision points evolve continuously. PIRs must evolve with them.

Why it fails. A static PIR list directs collection against requirements that may no longer be relevant while failing to address new requirements that have emerged. Collection assets are tasked against outdated questions; the commander's current intelligence gaps go unaddressed.

Correction. Review the PIR list at every intelligence synchronization meeting. For each PIR: Is the associated decision still pending? If yes, maintain the PIR active. If the decision has passed, close or suspend the PIR. Identify new intelligence requirements from the S3 and commander, and add them as PIRs on the collection plan. The PIR list is a living data product, not a planning document.

Failure Mode 3: Collection Gap Visibility Without Collection Gap Action

Description. The MSS collection management dashboard shows PIRs with no coverage — a gap is visible. The 35F notes the gap in the morning update. The same gap appears the next morning, and the next. No action is taken to fill the gap.

Cause. Collection gap identification is confused with collection gap resolution. MSS makes gaps visible; resolving them requires authority, coordination, and follow-through that the platform cannot provide.

Why it fails. A collection gap that is visible but unresolved is worse than a collection gap that is invisible — it means the intelligence section knows the PIR is unanswered and has chosen not to act. If the commander's decision fires on an unanswered PIR, the section has no basis for surprise.

Correction. Every collection gap identified on MSS must generate a specific action: retask an organic asset, submit an RFI to higher, or formally document that no collection is available and notify the S3/commander that the PIR cannot be answered through available means. "Identified" is not a disposition. Every gap must have an owner and a deadline.

Failure Mode 4: SIGACT Database Treated as a Reporting System, Not an Analytical Resource

Description. The 35F enters SIGACTs into MSS as a reporting function — capturing what happened for the record. Pattern analysis queries are rarely run. The SIGACT database grows without being analytically mined.

Cause. In a high operational tempo environment, the production cycle consumes all available analyst time. SIGACT entry is a required function; pattern analysis feels like additional work.

Why it fails. The SIGACT database is the primary historical record of enemy activity in the AO. Without regular pattern analysis, that record generates no intelligence. The commander receives a list of individual SIGACTs rather than an analytical assessment of what they collectively indicate about enemy intent and preparation.

Correction. Assign pattern analysis as a named task with a defined frequency — not less than weekly, more often in high-tempo environments. The output of pattern analysis is a product that goes to the section chief and into the INTSUM, not a note in an analyst's notebook. Pattern analysis is not optional; it is a core intelligence analytical function.

Failure Mode 5: HUMINT Source Data Boundary Erosion

Description. Under time pressure, HUMINT reporting entering MSS includes source-identifying information — descriptions of source characteristics, meeting location patterns, or language that would allow a reader to identify the source from available information.

Cause. The distinction between intelligence reporting and source management data can blur under production pressure, particularly when 35M collectors are entering their own reports rather than routing through 35F and 35D review.

Why it fails. Source identity exposure is a catastrophic intelligence failure with potentially lethal consequences. There is no operational tempo justification for source exposure. A single HUMINT source who is identified and eliminated cannot be replaced by any platform capability.

Correction. All HUMINT entries into MSS must go through 35F review before publication. The 35F is responsible for sanitizing source-identifying information before any HUMINT-derived content appears in MSS. This review step is non-negotiable and must be reflected in the section SOP. Coordinate with the HOC on specific sanitization standards.

Failure Mode 6: IPB Products Treated as Complete Upon Publication

Description. The MCOO, event template, and DST are built during planning, published to MSS, briefed to the commander, and then not updated as new collection arrives. When the operation executes, the intelligence section is working off IPB products that may be days or weeks out of date.

Cause. IPB production during MDMP is resource-intensive. Once the products are complete and approved, there is natural resistance to revisiting them — they represent significant analytical investment, and updating them requires additional work.

Why it fails. The enemy does not remain static after the OPORD is issued. Terrain conditions change. Enemy positions shift. New collection changes the threat assessment. IPB products that do not reflect current collection are worse than no IPB at all — they give the commander false confidence in an outdated picture.

Correction. Assign update triggers to every IPB product in MSS. Document the trigger conditions: "MCOO updates when bridge status changes, when new obstacle reporting arrives, or after 7 days regardless of new collection." Document the owner — which analyst is responsible for each product's currency. When a trigger fires, the update happens immediately, not at the next planning cycle.

Failure Mode 7: Cross-Echelon Intelligence Product Duplication Without Integration

Description. BCT S2 produces a SIGACT overlay. Division G2 produces a separate SIGACT overlay using the same underlying data plus Division-level collection. Corps ACE produces a third. Each echelon is working from a slightly different picture without visibility of what the other echelons have assessed from the same data.

Cause. MSS enables vertical access — BCT can see Division products; Division can see Corps products. But without deliberate cross-echelon product integration, analysts default to producing their own products from their own data rather than building on what already exists.

Why it fails. The intelligence picture fragments along echelon lines. BCT S2 may reach different conclusions about OPFOR intent than Division G2 using the same underlying data — not because of different collection but because of siloed analysis. This fragmentation is operationally dangerous when BCTs are making decisions about direct contact with the enemy based on a threat picture that diverges from the Division's assessment.

Correction. Establish a vertical product integration standard in the unit SOP: BCT INTSUM must explicitly reference and reconcile any differences with the supporting Division G2 assessment. Division G2 must review BCT SIGACTs for patterns not visible at Division level before publishing the Division INTSUM. Intelligence products on MSS should build vertically, not independently. Use the platform's shared workspace capability to make cross-echelon coordination a structured process, not an ad hoc conversation.

SECTION 8 — THE INTELLIGENCE-FIRES INTEGRATION MENTAL MODEL

BLUF: Intelligence and fires are the most tightly coupled WFF pair in the targeting cycle. The D3A methodology requires intelligence to both feed and close the targeting loop. MSS enables this integration through a shared data environment — but the integration must be designed and validated before it is needed, not constructed during a targeting event.

8-1. D3A as a Shared Data Loop

The Decide-Detect-Deliver-Assess cycle is not a sequential handoff — it is a concurrent shared data environment. While intelligence is detecting a target, fires is planning the attack. While fires is delivering, intelligence is preparing to assess effects. While intelligence is assessing, targeting is deciding re-attack criteria.

This concurrency requires that intelligence and fires share a live, common data environment — not exchange products at handoff points. MSS provides this environment through the shared targeting workspace. But shared environment is a necessary precondition, not a sufficient one. The data ownership boundaries, update standards, and escalation procedures that make the shared environment functional are human agreements that the targeting officer and G2/S2 must establish before operations.

The three data boundaries in a targeting workspace:

- **Intelligence boundary.** Intelligence section owns: target identification and analysis, locating data, pattern of life, HVT/HPT analytical assessment, and BDA intelligence collection. Only intelligence writes to these fields.

- **Fires boundary.** Fires section owns: attack system assignment, munitions selection, effects assessment, deconfliction, and re-attack recommendations. Only fires writes to these fields.
- **Command boundary.** Targeting officer and commander own: target approval, prosecution criteria, ROE application, and attack authorization. These decisions are documented in the workspace but made by authority, not by platform function.

When data ownership boundaries are unclear, the targeting workspace degrades. Both sections edit the same field. Neither section updates a field because each assumes the other is responsible. The result is a targeting product that appears complete but contains unverified data.

NOTE: The intelligence-fires data boundary is not negotiable based on time pressure. When a time-sensitive target emerges, the temptation to blur data ownership boundaries increases. Resist it. A target location entered by fires personnel without intelligence validation is an unvalidated target location — regardless of the urgency. The standard does not change; the speed of applying it must.

8-2. BDA as the Intelligence Anchor in the Targeting Cycle

Battle Damage Assessment closes the D3A loop. It is the phase where the intelligence cycle restarts — collection determines whether the target was physically, functionally, and systemically destroyed, or whether re-attack is required.

The most common BDA failure mode on MSS is treating BDA as a fires function rather than an intelligence function. Fires records strike execution. Intelligence assesses effects. These are different functions requiring different data. A BDA entry that records only strike time and munitions used is a strike record, not a BDA — it tells the commander what was delivered, not what was achieved.

The intelligence section's BDA discipline determines the quality of the targeting cycle assessment. A targeting cycle with disciplined BDA — physical, functional, and system effects assessed from multiple collection sources, confidence-rated and dated — gives the targeting officer a basis for re-attack determination. A targeting cycle with poor BDA forces the targeting officer to make re-attack decisions based on assumptions rather than assessment.

8-3. Pre-Operation Integration Validation

The Appendix D checklist in SL 4A exists because targeting workspace access failures are preventable. The most common access failure pattern: the unit has been using MSS for weeks, a time-sensitive targeting event occurs, and the fires cell does not have access to the target object that the intelligence section has been maintaining. The target exists in MSS; the fires cell cannot see it.

The antidote is a formal integration validation — every access point in the targeting workspace tested with actual personnel before operations begin. Not assumed. Not assigned. Tested. The targeting officer who validates the workspace access checklist before the first targeting event will not face an access gap during a time-sensitive targeting cycle.

SECTION 9 — INTELLIGENCE OPERATIONS IN A CONTESTED DATA ENVIRONMENT

BLUF: A sophisticated adversary will attempt to degrade, deny, deceive, or corrupt the data environment that MSS depends on. Intelligence practitioners must understand how adversary influence against the data layer threatens intelligence operations, and how doctrinal principles protect against it.

9-1. The Data Layer as an Adversary Target

MSS's value to intelligence operations is also its vulnerability. The platform integrates data from multiple sources into a common environment. If an adversary can corrupt that data — injecting false reporting, manipulating collection feeds, or deceiving the sources whose reporting enters MSS — the integrated product becomes a vehicle for systematic deception.

Adversary action against the data layer can take several forms:

- **Source manipulation.** A controlled or deceived HUMINT source provides false reporting that enters MSS as validated collection. The integrated picture reflects the adversary's desired narrative rather than reality.
- **Physical collection denial.** The adversary conceals, disperses, or deceives GEOINT and SIGINT collection assets, causing collection feeds to show absence of activity where activity is actually occurring.
- **Electronic warfare against data pipelines.** Adversary EW operations may degrade SIGINT feeds, disrupt data transmission, or create false signal signatures that enter the data environment as collection.
- **Cyber intrusion.** Adversary cyber operations targeting MSS or its data feeds could corrupt stored data, inject false objects, or manipulate historical records that the pattern of life baseline depends on.

The intelligence section cannot assume that the data in MSS is accurate simply because it is integrated. The analytical discipline of source evaluation, corroboration assessment, and alternative analysis is the defense against data layer attacks.

9-2. Protecting the Analytical Picture Against Deception

Indicators of adversary influence against the data layer:

- Collection reporting from multiple sources that is internally consistent to an unusual degree — adversary deception operations are frequently "too clean," lacking the normal noise and contradiction of genuine intelligence

- Collection gaps that appear in specific areas immediately before anticipated operations — adversary collection denial operations often produce systematic blanks in the GEOINT/SIGINT picture
- Pattern of life baselines that shift suddenly and simultaneously across multiple NAIs — may indicate an adversary operational security measure rather than genuine behavior change
- HUMINT reporting that aligns precisely with GEOINT observations in ways that seem unlikely given the source's access — may indicate fabrication or feed manipulation

When these indicators appear, the appropriate response is an analytical red team review — explicitly examining the hypothesis that the integrated picture reflects adversary deception, not just an aggregation of valid reporting.

9-3. Doctrinal Protections Against Data Layer Attacks

The doctrinal protections against adversary data layer manipulation are the same protections that have always governed intelligence analysis:

- **Source reliability evaluation.** A deceived or controlled source fails source reliability criteria when their reporting is examined against historical performance and access. Maintain rigorous source reliability records.
- **Independent corroboration.** Require that consequential intelligence assessments be corroborated by sources that are independent — not just reports from the same source processed through different channels.
- **Alternative analysis.** Explicitly examine the hypothesis "the adversary is deceiving us" before making a high-confidence assessment. This is not pessimism — it is analytical discipline.
- **PACE plan for data.** Maintain the ability to operate without MSS and without the data feeds that feed MSS. An intelligence section that can conduct IPOE from raw collection, without MSS integration, cannot be fully disabled by adversary action against the data layer.

NOTE: FM 2-0 identifies "vulnerability to deception and manipulation" as a fundamental characteristic of intelligence (FM 2-0, para 1-12). MSS does not eliminate this vulnerability. The more data MSS integrates, the more consequential a systematic deception operation can be. Analytical skepticism is a force protection function, not an obstacle to production speed.

SECTION 10 — THE ANALYST'S RELATIONSHIP WITH THE PLATFORM

BLUF: How an analyst thinks about MSS — the mental posture they bring to the platform — determines whether MSS improves analytical output or creates new failure modes. This section addresses the analyst's professional relationship with a data platform and the discipline required to use it well.

MSS as a Tool, Not an Authority

Every tool shapes the thinking of those who use it. A commander who relies entirely on the COP for situational awareness gradually stops looking out the window. An analyst who relies entirely on MSS for the intelligence picture gradually stops questioning whether the picture is complete.

The appropriate mental posture toward MSS: the platform is a high-quality tool that significantly aids the intelligence function. It is not an authority. An MSS dashboard that shows "no activity" in a NAI does not mean the enemy has no activity there. It means no reporting has been received from that area and ingested into MSS. The distinction is analytically significant.

This discipline — distinguishing between "the data shows X" and "the situation is X" — is the most important mental habit an intelligence analyst can develop when working in a data-rich environment. MSS makes this discipline harder because the data environment is so integrated and comprehensive that the absence of data becomes less visible. A manual system has obvious gaps — blank pages in the report book. MSS has invisible gaps — PIRs with no collection coverage look similar on the dashboard to PIRs with partial coverage.

NOTE: FM 2-0 describes the analytical process as "analysis and conversion of processed information into intelligence" (FM 2-0, para 2-21). The key word is "conversion" — not "display." An analyst who displays MSS data without converting it through analytical judgment has not completed the analytical task. The conversion step is human and non-delegable.

The Expertise Gradient

Not all intelligence practitioners bring the same analytical expertise to MSS. The platform is equally accessible to a first-tour 35F and a senior 35D with fifteen years of all-source experience. MSS does not filter by expertise. The commander receives products from both.

This creates a risk: MSS can make analytically weak products look like analytically strong products. A well-formatted INTSUM dashboard with current data, clean visualization, and professional layout looks authoritative regardless of the analytical quality of the assessment text. Section chiefs must look past the formatting and read the assessment: Is there a stated confidence level? Is there an alternative explanation addressed? Is the analytical reasoning explained, or is the product simply a data summary with a conclusion attached?

The section chief's role in an MSS environment is to ensure that products reflect genuine analysis, not data display. This requires reading the assessment text, not just reviewing the dashboard layout.

The Analyst as Data Steward

Every analyst who enters data into MSS is a data steward for the formation. The SIGACT entered today will be used by analysts tomorrow, next week, and in the next rotation. The quality of the data entered — complete source attribution, accurate grid coordinates, correct activity taxonomy, validated source

reliability rating — determines the quality of the historical record that subsequent analysts work from.

This stewardship responsibility is not instinctive in an environment where the immediate pressure is the next BUA brief, not the quality of the historical record. Section chiefs must enforce data stewardship standards explicitly and consistently.

Table 8-1. Data Stewardship Standards by Object Type

Object Type	Most Common Error	Impact	Standard
Activity event / SIGACT	Missing source reliability rating	Pattern analysis built on unrated sources has no analytical confidence foundation	Enforce before workspace publication
Threat unit location	6-digit MGRS instead of 10-digit	1,000m location uncertainty propagates into targeting and COA analysis	10-digit MGRS required for all tactical-level locations
PIR status	Not updated after decision has passed	Stale PIRs drive collection against obsolete requirements	Review and update at every intelligence synchronization meeting
HUMINT contact report	Source-identifying descriptor included	Source exposure risk	35D review required before any HUMINT object is published
COA overlay	Not versioned on significant update	Previous analytical position lost; audit trail broken	Version increment required on all significant COA assessment changes

SECTION 11 — INTELLIGENCE LEADERSHIP AND MSS GOVERNANCE

BLUF: MSS introduces governance responsibilities that did not exist — or were simpler — in a manual intelligence environment. The section chief is simultaneously an operational leader, an analytical quality reviewer, and a data governance authority. This section addresses the leadership dimension of MSS employment.

The Section Chief as Data Governance Authority

In the MSS environment, the intelligence section chief (35X, S2, or G2) holds three concurrent roles: operational leader, analytical product quality authority, and data governance authority. The governance role is new. Most section chiefs received no explicit preparation for it.

Data governance for the intelligence section on MSS includes: - Determining what data enters intelligence workspaces and what does not - Setting and enforcing data quality standards for all object types - Managing workspace access and need-to-know determinations - Reviewing audit logs for access anomalies - Approving all products before distribution outside the section - Establishing and enforcing the update cycle for every living product

These functions cannot be fully delegated. The section chief must own them even when analysts perform day-to-day execution. An access anomaly in the HUMINT workspace is a section chief problem — not an MSS administrator problem.

Product Approval Authority

Every intelligence product published on MSS for distribution outside the intelligence section requires section chief approval. Time pressure is not a reason to skip product approval — it is a reason to streamline the approval process. Streamlining options include: pre-approved product templates with defined data fields, standing approval authority for defined routine products at steady state, and MSS workflow routing that formalizes the approval sequence.

What does not constitute a streamlining option: analysts publishing products without section chief review because the section chief is busy. This removes the quality control mechanism that protects the commander from analytically unsound intelligence products.

Managing the Intelligence Picture Across Rotations

Personnel rotations are endemic to Army operations. In an MSS environment, the incoming analyst inherits the entire historical workspace — all of the outgoing analyst's data, products, and assessments. This is a continuity improvement. It is also a risk: the incoming analyst may accept the inherited picture without critically reassessing the analytical baseline.

Incoming section chiefs and senior analysts should conduct a deliberate workspace review at the start of each rotation: validate threat assessments against current collection, check product update cycles, review data quality standards, and confirm that access controls reflect the current personnel roster. The inherited workspace is a starting point, not an authoritative fact pattern.

NOTE: A threat assessment in MSS that was analytically sound six months ago may be analytically unsound today if the threat has evolved and the workspace has not been updated to reflect new collection. Inheriting a workspace does not mean inheriting the analytical validity of its contents. Section chiefs are responsible for the current accuracy of every product in the workspace under their authority, regardless of when it was originally built.

CLOSING NOTE

This guide has established the conceptual framework for Intelligence WFF practitioners using MSS. The central themes:

- MSS is a data integration platform. Intelligence is an analytical discipline. Both are required. Neither replaces the other.
- The intelligence process (FM 2-0) is the governing framework. MSS improves each phase; it does not change which phases exist or what each phase requires.
- IPB is a continuous process. MSS enables continuous IPB; the discipline to maintain living products must come from the section leadership.
- Collection management data discipline determines whether MSS improves or merely documents the intelligence failure.
- All-source fusion is a human analytical function. Co-located data is a necessary but not sufficient condition for finished intelligence.
- Classification and OPSEC discipline on MSS is a force protection function, not just a compliance function.

When you encounter a difficult situation using MSS in an intelligence role — a product that does not exist, a data feed that is stale, a collection gap that cannot be filled — apply the doctrinal framework first. What phase of the intelligence process is affected? What product standard applies? What is the fallback procedure? The answers are in FM 2-0, ATP 2-01.3, ATP 2-01, and SL 4A. MSS is the tool. The doctrine and the tradecraft are the profession.

RELATED TRACKS AND PUBLICATIONS

WFF Peer Tracks

All six WFF tracks are at the same tier. All six WFF tracks require SL 1, SL 2, and SL 3 as prerequisites. Intelligence practitioners are encouraged to develop working awareness of peer WFF tracks, particularly fires and mission command, where data integration with intelligence is most intensive.

Track	Title	Prereq	Relationship to Intelligence WFF
SL 4A	Intelligence WFF	SL 1 + SL 2 + SL 3	This track

Track	Title	Prereq	Relationship to Intelligence WFF
SL 4B	Fires WFF	SL 1 + SL 2 + SL 3	Targeting data, AMD coordination, fires-intel integration — see Section 8 of this guide
SL 4C	Movement and Maneuver WFF	SL 1 + SL 2 + SL 3	NAI/TAI overlays, reconnaissance data feed into M&M operations process
SL 4D	Sustainment WFF	SL 1 + SL 2 + SL 3	LOC threat data, supply point security — intelligence supports sustainment planning
SL 4E	Protection WFF	SL 1 + SL 2 + SL 3	AT intelligence integration; threat data for AT assessments
SL 4F	Mission Command WFF	SL 1 + SL 2 + SL 3	PIR-derived CCIR components feed commander's CCIR dashboard — primary coordination partner

Specialist Tracks (Prerequisite: SL 3)

For personnel pursuing technical depth beyond WFF employment, the specialist tracks (SL 4G–O, prereq SL 3) are available. GEOINT and SIGINT data management practitioners may find SL 4H (AI Engineer) and SL 4M (ML Engineer) relevant for advanced analytical capability development.

Track	Title
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)
SL 4N	UI/UX Designer (→ SL 5N)
SL 4O	Platform Engineer (→ SL 5O)

NOTE — New Doctrine Content in SL 4A: SL 4A now includes an FM 2-0 data literacy call-out validating this training, an intelligence process→data pipeline mapping table (Table 1-1a), and seven characteristics of effective intelligence as data quality standards (Table G-0a, FM 2-0). These sections ground the concepts in this guide in their authoritative doctrinal sources.

This publication supersedes all previous versions. The proponent agency for CONCEPTS_GUIDE_TM40A is the USAREUR-AF C2 Data and Analytics Office (C2DAO), Wiesbaden, Germany.

For questions or recommended changes to this publication, contact the C2DAO publications manager through the unit S6 or G6.