DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

TECHNICAL MANUAL

SL 1

USAREUR-AF

TM-10 — MAVEN SMART SYSTEM (MSS)

User/Operator Manual

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

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

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

TM-10 — MAVEN SMART SYSTEM (MSS)

Foreword: This manual tells you how to use the Maven Smart System (MSS) as a data consumer. It covers logging in, finding your unit's information, reading dashboards, submitting forms, and staying within authorized boundaries. No technical background is required. You do not need to know how to write code or build anything. If you can use a smartphone or a web browser, you can use MSS. **Proponent:** USAREUR-AF Operational Data Team (ODT) **Prereqs:** None (formal). Data Literacy Technical Reference (recommended prior reading — not required). *HQ USAREUR-AF · v1.0 · 2026 · DISTRIB: USG only · AUTH: C2DAO/UDRA v1.1*

TABLE OF CONTENTS

CHAPTER 1 — INTRODUCTION AND OVERVIEW

1-1. USER/OPERATOR MANUAL

This Technical Manual (TM) provides operator-level instruction for the Maven Smart System (MSS). It is written for all USAREUR-AF military personnel (officer, warrant, NCO, and enlisted) and DA Civilians and Contractors who access MSS in the course of their duties.

This manual covers what you need to use MSS as a consumer of data logging in and navigating the platform; finding and reading dashboards and reports; submitting information through forms; executing authorized actions; working with data in analysis tools; using AI assistant tools; handling data securely and within your authorization; and troubleshooting common problems.

This manual does NOT cover building applications or dashboards; creating or modifying data pipelines; writing any code; configuring the platform in any way; or designing AI workflows.

Those tasks are covered in SL 2 (Workshop Builder) and SL 3 (Advanced Builder). If a task you need to perform is not in this manual, contact your unit data steward before attempting it.

NOTE

If a task in this manual indicates it requires a builder or engineer, do not attempt it yourself. The escalation path is: (1) SL 1 operator attempt fails or is out of scope → (2) Contact your unit data steward → (3) Data steward routes to SL 2 builder (Workshop apps, basic pipelines, Ontology configuration) or SL 3 advanced builder (complex design, AIP Logic, enterprise Ontology) or SL 4 developer (code required). Chapter 7 of this manual contains the full escalation decision guide.

1-2. WHAT THE MAVEN SMART SYSTEM IS

MSS is the mission command information system (MCIS) program of record, directed by the USAREUR-AF CG to enable rapid and accurate decision-making. It is a secure, web-based platform where your unit's operational data lives. Think of it like a shared operations center for information: data from logistics, personnel, readiness, and other Army systems is collected, organized, and made visible through applications your unit uses every day.

MSS is built on the Palantir Foundry software platform, authorized for Army use under the Maven Smart System program. When you log into MSS, you are logging into Foundry with Army data and Army-controlled access.

Per ADP 3-13, information is combat power. MSS is the USAREUR-AF platform for converting raw data into the operational information commanders and staff need to make decisions and maintain decision dominance across the European theater.

> **NOTE**
>
> In emerging Army terminology, the applications you use on MSS are sometimes called **Automated Fighting Products (AFPs)** — staff and leader data visualization tools connected to live data via automated pipelines that reduce the time required to produce running estimates and inform commander decision-making. The data you see in an MSS dashboard is **operationalized data** — data analyzed and presented to be immediately actionable. Every time you open a dashboard, you are consuming an AFP built from operationalized data. The training program that teaches you to use, build, and maintain these AFPs is the MSS curriculum you are beginning now. *(AFP terminology from Adkins, "Achieving Decision Dominance," Military Review, January-February 2025 — a thought piece proposing these concepts.)*

What MSS does stores data from Army systems (GCSS-A, DCPDS, MEDPROS, unit feeds, and others) in one organized place; makes that data visible through applications any Soldier can use without technical training; allows units to report status, update records, and track readiness through those same applications; provides analysis tools for personnel who need to look at data in more depth; and supports AI-assisted analysis through authorized tools.

What MSS is NOT it is not a replacement for official Army systems of record — MSS reads from those systems but does not replace them; it is not classified by default — the classification of data in MSS depends on what data is loaded and how it is marked; or a public system — access is tightly controlled and every action is logged.

1-2A. THE COGNITIVE HIERARCHY — WHY DATA MATTERS

Army doctrine (ADP 6-0, ADP 3-13) defines a four-level hierarchy that explains how raw data becomes the understanding commanders need to make decisions:

Level	Definition	MSS Example
Data	Unprocessed signals; numbers, text, sensor readings	A feed of GCSS-A equipment status codes arriving in MSS
Information	Data organized to provide context and meaning	A dashboard showing "V Corps has 847 NMC vehicles by type"

Level	Definition	MSS Example
Knowledge	Information analyzed to reveal patterns and significance	An analyst's assessment that NMC rates in 2CR spiked 40% after rotation
Understanding	Knowledge with judgment applied to comprehend the situation	The G4's determination that current NMC trends will degrade readiness below C2 within 60 days unless parts flow increases

Per ADP 3-13, information is a dynamic of combat power — at the same level as firepower, mobility, and survivability. MSS automates the lower tiers of this hierarchy (data → information) so humans can focus on the higher tiers (knowledge → understanding). That is why you are learning this platform.

1-2B. THE GMAD FRAMEWORK — A DOCTRINAL MENTAL MODEL FOR DATA PLATFORMS

The Geospatial Engineer's GMAD framework — Generate, Manage, Analyze, Disseminate — defined in FM 3-34 (Engineer Operations) provides the closest existing Army doctrinal analog to how a data platform operates. Although GMAD was written for geospatial engineering, the four functions map directly to MSS and give every operator a simple, doctrine-grounded way to think about what the platform does.

Table 1-1a. GMAD Framework Applied to MSS

GMAD Function	Data Platform Equivalent
Generate	Data ingestion — collecting and importing data from source systems (GCSS-A, DCPDS, MEDPROS, unit feeds)
Manage	Data governance — storing, cataloging, securing, and maintaining data within the platform
Analyze	Data analysis — transforming data into information and insights through pipelines, dashboards, and AI tools
Disseminate	Data publication — sharing products with authorized consumers through Workshop applications and exports

NOTE

You do not need to memorize this framework. It is provided so you understand that MSS is not a novel concept — it follows the same doctrinal logic the Army already uses for managing geospatial products. The platform generates data, manages it under governance, analyzes it into useful products, and disseminates those products to the people who need them. (Source: FM 3-34, Engineer Operations.)

1-2C. THE OPERATIONS PROCESS — WHERE MSS FITS

The Army's operations process — Plan, Prepare, Execute, Assess (ADP 5-0, FM 5-0) — is the overarching cycle that generates and consumes data products. MSS supports all four phases:

Operations Process Phase	How MSS Supports It
Plan	Commanders and staff access readiness dashboards, logistics status, and personnel data to develop courses of action
Prepare	Units use MSS to track task completion, verify resource availability, and confirm force posture before execution
Execute	Operators submit SITREPs, update status, and monitor operations through MSS applications in near-real time
Assess	Leaders review dashboards and reports to evaluate progress, identify variances, and adjust operations

Every data product in MSS exists to support one or more phases of this cycle. When you open a dashboard, you are participating in the operations process — even if your task feels routine.

1-2D. METT-TC(I) — DATA IS NOW IN EVERY MISSION VARIABLE

NOTE

The 2025 update to Army doctrine (ADP 3-0, FM 3-0) added "Informational considerations" as a parenthetical to every mission variable. METT-TC becomes METT-TC(I): Mission, Enemy, Terrain and weather, Troops and support available, Time available, Civil considerations — and now Informational considerations. This means data and information are doctrinally embedded in ALL planning factors, not just intelligence. Every MSS user operates within this framework. When a commander analyzes the operational environment using METT-TC(I), the "(I)" includes the data products you access, create, and report through MSS. Accurate, timely data in the platform directly supports the informational dimension of every mission variable.

1-3. MSS IN THE USAREUR-AF CONTEXT

United States Army Europe and Africa (USAREUR-AF) is the Army Service Component Command (ASCC) for United States European Command (USEUCOM) and United States Africa Command (USAFRICOM). USAREUR-AF coordinates theater land operations across the European and African Areas of Responsibility (AOR), integrates with NATO Allied commands, and contributes to Joint All-Domain Command and Control (JADC2). The command operates across multiple countries and time zones — including Germany, Poland, Romania, and the Baltics — coordinating with III Corps, V Corps, 21st Theater Sustainment Command (TSC), 7th Army Training Command (ATC), 10th AAMDC, 56th MDC-E, SETAF-AF, and numerous Allied and partner nation forces.

MSS is USAREUR-AF's primary data and AI platform. It serves as the command's single integrated environment for theater readiness visibility, logistics status, personnel accountability, and operational reporting. MSS is not a standalone tool — it is the data backbone that supports decision-making from battalion staff through theater army.

Table 1-1. MSS Mission Areas in USAREUR-AF

Mission Area	Example Use
Personnel Readiness	Viewing and reporting Soldier readiness status across subordinate units
Logistics	Tracking equipment availability and maintenance status for V Corps and 21st TSC
Operational Reporting	Submitting and viewing SITREPs from units in Poland and Romania
Command & Control	Tracking unit task organization and positioning across the AOR
NATO Integration	Sharing approved data products with Allied partners via authorized channels
Exercise Support	Monitoring readiness and force generation status during DEFENDER-series exercises

Your access level and the applications available to you depend on your assigned role and markings. An S2 section in Poznan will see different applications and data than an S4 shop in Grafenwoehr — that is by design.

1-3A. THE OPERATIONAL DATA TEAM — WHERE MSS CAPABILITY COMES FROM

The applications and data products you use on MSS do not appear by themselves. They are built and maintained by **Operational Data Teams (ODTs)** — multifunctional teams of product managers, UX designers, software engineers, data engineers, and data scientists who work together to solve

operational problems with data.

The ODT concept was first piloted by XVIII Airborne Corps beginning in 2022. XVIII ABC published its experience — including organizational lessons learned and the manning structure they arrived at — in *Military Review* (February 2026). The Mission Command Center of Excellence (MCCoE) has since codified ODT organization and echeloned employment in the **Decision Optimization Concept of Operations**, and SEC ARMY directed Army-wide experimentation under Transformation in Contact 2.0. USAREUR-AF's own ODT predates the XVIII ABC publication and operates under the C2DAO with a theater-specific organizational model. The XVIII ABC experience is a reference point — not a template — and different commands will adapt the concept to their own mission, manning, and echelon. Notably, LTG Donahue, who directed the original Data Warfare Company activation at XVIII ABC in 2022, now commands USAREUR-AF.

Why this matters to you as an MSS user: The ODT is the team that builds the dashboards you read, the forms you submit, and the tools you use. When you encounter a data problem, a broken application, or a requirement for a new capability, the escalation path leads to the ODT. Understanding that these tools are built by a trained, organic team — not a vendor or a help desk — helps you route requests effectively and set realistic expectations for new capability delivery.

USAREUR-AF's Operational Data Team operates under the C2DAO with direct alignment to theater strategy. The MSS training curriculum (SL 1 through SL 5) is the pipeline that produces the qualified personnel who staff ODTs at every echelon — from the Theater Army Operational Data Section down through subordinate Corps and Division ODTs.

NOTE

The MSS specialist tracks (SL 4J through SL 4O) map directly to the ODT roles employed by XVIII ABC in their pilot: Product Manager (SL 4J), UX Designer (SL 4N), Software Engineer (SL 4L), Data Engineer (SL 3/SL 4K), and Data Scientist (SL 4G/SL 4M). If your career path leads toward one of these roles, the MSS training curriculum is your qualification pathway.

In February 2026, the Combined Arms Command at Fort Leavenworth began formally integrating Maven into institutional training and professional military education. MCCoE senior instructors are developing a standardized 8-hour hands-on operator course; the Command and General Staff College is incorporating Maven into core curriculum for field grade officers; and the CAC Data Academy is offering a Low-Code/No-Code Builders Course. This means the institutional Army is now building toward the same competencies this training program delivers — the MSS curriculum (SL 1 through SL 5) prepares you for tools and skills the Army is scaling enterprise-wide.

Sources: Forney, Herrmann, and Steele, "Fighting with Live Data," Military Review Online Exclusive, February 2026; MCCoE Decision Optimization CONOPS, Appendix B; "Army's Combined Arms Command to integrate Maven C2 smart system into training and education," army.mil, February 2026.

1-4. GOVERNANCE CHAIN AND POLICY REFERENCES

Data governance in USAREUR-AF flows through a defined chain of authority. Knowing this chain tells you who to contact when you have a problem, a question, or need access.

Governance chain (top to bottom):

```
DoD CIO / CDAO
        ↓
Army CIO / Mission Area Data Officers (MADOs)
        ↓
DoD Data Strategy (VAULTIS framework) / DDOF Playbook v2.2 (VAULTIS-A)
        ↓
Army CIO Data Stewardship Policy (April 2, 2024)
        ↓
USAREUR-AF Command Chief Data & Analytics Officer (C2DAO)
        ↓
Functional Data Managers (by domain: personnel, logistics, ops)
        ↓
Unit Data Stewards
        ↓
MSS Users (you)
```

Governing references:

- **AR 25-1, Army Information Technology (Jul 2019)** — statutory framework for Army data governance and IT management policy. Established the original VAUTI (5-dimension) data quality principles at the Army level. NOTE: VAUTI has been superseded by VAULTIS (7 dimensions — DoD Data Strategy 2020) and extended to VAULTIS-A (8 dimensions — DDOF Playbook v2.2, December 2025) which adds Linked, Secure, and Auditable. VAULTIS-A is the current operational quality gate for all MSS data products.
- **ADP 3-13, Information** — establishes information as a warfighting function and the foundation for understanding MSS's role in USAREUR-AF operations.

> **NOTE**
>
> The USAREUR-AF C2DAO office is responsible for implementing and enforcing Army data policy within this command. For governance questions, access exceptions, or policy issues, contact the C2DAO office through your chain of command.

DoD and Army Strategic References:

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

- **DoD Data Strategy (October 2020)** — Establishes the VAULTIS framework (Visible, Accessible, Understandable, Linked, Trustworthy, Interoperable, Secure) as the DoD standard for data quality.

Supersedes the 5-dimension VAUTI model from AR 25-1.

- **DDOF Playbook v2.2 (December 2025)** — T2COM C2DAO implementing document. Extends VAULTIS to VAULTIS-A (adds Auditable as 8th dimension). Establishes 85% minimum weighted average across all 8 dimensions as the quality gate for DDOF Phase 3. This is the authoritative standard for MSS data product quality.
- **Army Data Plan (2022)** — 11 strategic objectives for Army data transformation
- **Army Cloud Plan (2022)** — Zero Trust, secure development, data-driven decisions
- **Army CIO Data Stewardship Policy (April 2, 2024)** — establishes the stewardship hierarchy and data chain of responsibility

---

1-5. PREREQUISITES — WHAT YOU MUST HAVE BEFORE USING MSS

Required before first login:

1. **Annual Cyber Awareness Training** — required for all DoD personnel with network access. You must complete this before your account will be activated.
2. **Provisioned MSS Account** — your unit S6 or data steward must submit a request and have it approved. You cannot create your own account.
3. **MSS User Onboarding Brief** — provided by your unit data steward or G6/S6. Covers your unit's specific applications and data.
4. **CAC reader and approved workstation** — MSS runs in a web browser. You need a working CAC reader and an approved government workstation.

Recommended (not required) prior reading: - Data Literacy Technical Reference - Supplemental training materials available through your unit data steward or C2DAO

Account provisioning takes 3 to 5 business days. If you have an upcoming deployment, exercise, or TDY requiring MSS access, start the account request process early.

1-6. SECURITY RESPONSIBILITIES — EVERY MSS USER

Every person who uses MSS is personally responsible for the items below. These are not optional. They apply whether you are a private first class in Baumholder or a colonel on the USAREUR-AF staff.

1. **Use only your own credentials.** Do not share your CAC, PIN, or any session token with anyone for any reason.

2. **Access only the data you are authorized to view.** Do not attempt to open projects, datasets, or applications that have not been granted to you.
3. **Report misrouted data immediately.** If you see data at a higher classification level than your clearance, stop and report it. Do not read it, copy it, screenshot it, or act on it.
4. **Do not export data without authorization.** All exports are logged. Downloading data to an unauthorized location is a security violation.
5. **Log out when you are finished.** Do not leave an MSS session open on an unattended workstation. **Logout procedure:** (1) Click your Profile icon in the upper right corner. (2) Select Log Out from the dropdown. (3) Wait for the login screen to confirm sign-out. (4) Close the browser tab. (5) Lock your workstation (Windows key + L).
6. **Report incidents.** If you suspect a security violation — yours or someone else's — report it to your supervisor and unit security officer immediately.

WARNING

Unauthorized access to, disclosure of, or modification of data in MSS may constitute a violation of 18 U.S.C. § 1030 (Computer Fraud and Abuse Act) and applicable Army regulations. Violations may result in loss of access, adverse action, and criminal prosecution.

1-7. HOW TO GET HELP

Table 1-2. Who to Contact for What

Problem Type	First Contact
Cannot log in	Unit S6/G6
Cannot access a project or dataset	Unit data steward
Data appears incorrect	Unit data steward
System error or application crash	USAREUR-AF MSS Help Desk (via unit S6/G6)
Security incident	Supervisor and unit security officer — IMMEDIATELY
Data governance or policy question	USAREUR-AF C2DAO office (via chain of command)

NOTE

Specific phone numbers and email addresses for MSS support contacts are maintained by your unit S6/G6. This manual does not list them because they change. Get current contact information from your S6/G6 or unit SOPs before you need them.

1-8. LOCATING SELF-PACED TRAINING MATERIALS

Self-paced training materials are available within MSS for operators who need to build or refresh skills outside of structured classroom instruction. These materials include walkthroughs, reference guides, and practice exercises that can be completed independently.

To find self-paced training resources, use the MSS Search bar (Chapter 3, Task 3-1) and search for terms such as "training," "self-study," or "MSS training." Training resources are typically organized within a designated training project folder managed by your unit data steward or the organizational data team.

NOTE — USAREUR-AF Example: Within USAREUR-AF, the Operational Data Team (ODT) maintains a self-paced training folder accessible via Compass. Search for "ODT Training" or ask your unit data steward for the current folder path. Other commands and organizations will have equivalent self-paced training resources with different names and locations. If you cannot locate training materials, contact your unit S6/G6 or data steward — do not assume they do not exist.

An MSS Training Hub application may also be available in your environment. The Training Hub provides a centralized view of training resources, self-study materials, and links to reference documentation. Ask your data steward whether this application has been published in your command's MSS environment.

1-9. HOW DATA REACHES YOU — A CONSUMER'S MENTAL MODEL

BLUF: Before you read a dashboard number and act on it, you need to understand where that number came from and what could make it wrong. This section gives you that mental model.

Every piece of information you see in MSS passed through a chain before it reached your screen. Understanding that chain is how you use data responsibly.

The chain, simplified:

```
SOURCE SYSTEMS          →    INTEGRATION          →    SEMANTIC LAYER          →    YOU
(GCSS-A, DCPDS,              (Pipelines process        (Ontology organizes           (Workshop
app
```

> MEDPROS, unit feeds) and clean the data) data as Objects) shows it to you)

1. **Source systems** — Army systems of record (GCSS-A for equipment, DCPDS for personnel, MEDPROS for medical readiness, and others) generate the raw data. MSS does not own this data. It reads it.
2. **Integration layer** — Automated pipelines ingest data from source systems on a schedule. This is not real-time. A pipeline that runs every four hours means the data you see may be up to four hours old. Currency varies by data domain — check your unit data steward if you need to know how fresh a specific feed is.
3. **Semantic layer (Ontology)** — Pipelines produce datasets that are organized into Object Types — structured representations of real things (a Soldier, a vehicle, a unit). The Ontology applies business rules, filters, and relationships. What you see has already been interpreted.
4. **Workshop application** — The application presents a filtered, designed view of Ontology data. The designer made choices about what to show and what to exclude. You are seeing a curated view, not all available data.

What this means when you read a dashboard:

If you see...	The likely cause
A number that seems wrong	Check when the data last refreshed before concluding the data is bad
A field showing "null" or blank	The source system may not have populated that field, or the pipeline hasn't run yet
A number that changed overnight	A scheduled pipeline ran and pulled updated source data — this is normal
Data that contradicts the system of record	The system of record is authoritative. Report the discrepancy to your data steward.

The most important habit: Before acting on a data product, know its currency (how old is it?) and its source (what system did it come from?). Both are visible in MSS — your data steward can show you where to find this information for each application you use.

NOTE

You are a data consumer, not a data validator. If something looks wrong, your job is to report it — not to correct it, work around it, or ignore it. The escalation path is in Table 1-2 (paragraph 1-7).

1-10. MSS TRAINING CURRICULUM — LEARNING PATH

SL 1 is the entry point for the MSS training curriculum. After completing SL 1, personnel may advance along one of two tracks depending on their role and assigned duties.

Advancement path:

Current Qualification	Next Step	Description
SL 1 (Operator)	SL 2 (Builder)	For personnel who have been granted builder access and will create pipelines, applications, or Ontology configurations. Prerequisite: SL 1.
SL 2 (Builder)	SL 3 (Advanced Builder)	For personnel who will design complex multi-source pipelines, advanced Ontology models, and multi-page applications. Prerequisite: SL 2.
SL 3 (Advanced Builder)	SL 4A — Intelligence WFF	For G2 / S2 staff applying MSS to intelligence workflows. Prerequisite: SL 3 (required). Duration: 3 days.
SL 3 (Advanced Builder)	SL 4B — Fires WFF	For fire support personnel applying MSS to fires workflows. Prerequisite: SL 3 (required). Duration: 3 days.
SL 3 (Advanced Builder)	SL 4C — Movement & Maneuver WFF	For G3 / S3 staff applying MSS to movement and maneuver workflows. Prerequisite: SL 3 (required). Duration: 3 days.
SL 3 (Advanced Builder)	SL 4D — Sustainment WFF	For G4 / S4 staff applying MSS to logistics and sustainment workflows. Prerequisite: SL 3 (required). Duration: 3 days.
SL 3 (Advanced Builder)	SL 4E — Protection WFF	For protection officers and NCOs applying MSS to force protection workflows. Prerequisite: SL 3 (required). Duration: 3 days.
SL 3 (Advanced Builder)	SL 4F — Mission Command WFF	For G6 / S6 and command staff applying MSS to mission command workflows. Prerequisite: SL 3 (required). Duration: 3 days.
SL 3 (Advanced Builder)	SL 4G — ORSA	For operational research and systems analysis specialists. Prerequisite: SL 3 (required). Duration: 5 days.
SL 3 (Advanced Builder)	SL 4H — AI Engineer	For personnel building and maintaining AIP Logic workflows and AI-enabled products. Prerequisite: SL 3 (required). Duration: 5 days.
SL 3 (Advanced Builder)	SL 4M — ML Engineer	For personnel developing machine learning pipelines and model integrations. Prerequisite: SL 3 (required). Duration: 5 days.
SL 3 (Advanced Builder)	SL 4J — Program Manager	For data program managers coordinating MSS products and delivery. Prerequisite: SL 3 (required). Duration: 4 days.

Current Qualification	Next Step	Description
SL 3 (Advanced Builder)	SL 4K — Knowledge Manager	For knowledge managers structuring data products for organizational learning. Prerequisite: SL 3 (required). Duration: 4 days.
SL 3 (Advanced Builder)	SL 4L — Software Engineer	For software engineers writing Python, PySpark, TypeScript, and OSDK integrations. Prerequisite: SL 3 (required). Duration: 5 days.
SL 3 (Advanced Builder)	SL 4N — UI/UX Designer	For personnel designing user interfaces and user experience for MSS applications. Prerequisite: SL 3 (required). Duration: 5 days.
SL 3 (Advanced Builder)	SL 4O — Platform Engineer	For personnel managing platform infrastructure, deployments, and environment configuration. Prerequisite: SL 3 (required). Duration: 5 days.
SL 2 (Builder)	T3-F — MSC Force Multiplier	Half-day Unit Data Trainer certification. Prereq: SL 2 Go + commander nomination. Authorizes SL 1 delivery and SL 1 exam proctoring.
SL 3 (Advanced Builder)	T3-I — Instructor Certification	5-day instructor pipeline course. Prereq: SL 3 Go + C2DAO Training OIC selection.
Any qualification level	EXEC — Senior Leader	For senior leaders (O-5 / E-9+). Provides data-informed decision-making framework without technical prerequisites. Duration: 1 day.

NOTE

Not every SL 1 graduate proceeds to SL 2. Most USAREUR-AF personnel require only SL 1 operator qualification to perform their duties. Builder access (SL 2 and above) is granted through chain-of-command request and requires explicit approval. If you believe your duties require builder access, speak with your unit data steward.

CHAPTER 2 — ACCESSING MSS

BLUF: This chapter walks you through logging in for the first time, what to do when you have problems logging in, and how to set up your account so it works for you.

> **NOTE**
>
> MSS implements Zero Trust Architecture (ZTA) per Army Unified Network Plan 2.0. Every access request is verified against your credentials and assigned markings. Sessions expire automatically and require re-authentication. This is normal and by design — it is not a system error.

TASK 2-1: SET UP YOUR ACCOUNT BEFORE FIRST LOGIN

CONDITIONS: Operator has received notification that an MSS account has been provisioned, has completed Cyber Awareness Training, has an active CAC, and has attended the unit MSS onboarding brief.

STANDARDS: Operator confirms account is active, collects the MSS portal URL and support contact information, and identifies the applications they are authorized to access.

EQUIPMENT: Active CAC, CAC reader, approved workstation, notification from MSS admin team, unit data steward contact information.

PROCEDURE:

1. Confirm you have received account activation notification from the MSS admin team or your data steward.
2. Obtain the MSS portal URL from your unit S6 or data steward. Write it down or save it — you will use it every time you log in.
3. Confirm your CAC reader is installed and working. Test by inserting your CAC and confirming your computer recognizes it (your computer may prompt for your PIN).
4. Confirm which browser to use. MSS works best on Google Chrome or Mozilla Firefox. Internet Explorer is not supported.
5. Ask your data steward: "Which applications am I authorized to use, and where are they?" Write down the names.
6. Keep your data steward's contact information available. You will need it if you have questions or problems.

7. **If you work on multiple enclaves (NIPR, SIPR, MPE, etc.), repeat steps 1–6 for each enclave.** Your MSS account on one enclave does not grant access on another. Each enclave requires separate account provisioning, a separate portal URL, and a separate first login. Confirm access on every enclave you need before relying on it operationally.

> **NOTE**
>
> Your unit data steward is your primary point of contact for everything related to your MSS access and the data you work with. If you do not know who your data steward is, ask your S6 or immediate supervisor.

TASK 2-2: LOG IN TO MSS

CONDITIONS: Operator has a provisioned MSS account, an active CAC, a working CAC reader, and an approved workstation with Google Chrome or Firefox installed.

STANDARDS: Operator successfully authenticates with CAC, reaches the MSS home screen, and can confirm their username is displayed correctly.

EQUIPMENT: CAC, CAC reader, approved workstation, MSS portal URL.

PROCEDURE:

1. Insert your CAC into the CAC reader.
2. Open Google Chrome or Firefox.
3. Type the MSS portal URL in the address bar and press Enter.
4. The browser will display a prompt asking you to select a certificate. **Select your authentication certificate** — it typically shows your name and DoD ID number. Do NOT select your email certificate.
5. Enter your CAC PIN when prompted. Type it carefully — three wrong PIN attempts will lock your CAC.
6. Wait for the MSS home screen to load. This may take 15 to 30 seconds.
7. Confirm your name or username appears in the upper right corner. If someone else's name appears, log out immediately and contact your S6.
8. Orient yourself to the home screen layout:
9. **Top navigation bar:** MSS/Foundry logo (far left — returns to home from anywhere), Search bar (center — fastest way to find any resource), Notification bell and Profile icon (far right).
10. **Left sidebar:** Compass icon (file browser for all MSS resources organized by project and folder).
11. **Main area:** Recently visited resources and pinned/starred items.
12. Click each navigation element once to see what it does. Do not submit any forms or execute any actions during this orientation step.

Table 2-1. MSS Navigation Elements at a Glance

Element	Location	What It Does
MSS/Foundry logo	Top left	Returns to home screen from anywhere
Search bar	Top center	Find any resource by name — fastest way to navigate
Notification bell	Top right	System alerts, workflow updates, reminders
Profile icon	Top right	Account settings, markings, logout
Compass (file browser)	Left sidebar	Browse all MSS resources organized by folder
Starred/Pinned items	Home screen	Shortcuts you have saved to frequently used resources
Recent activity	Home screen	Resources you visited recently

NOTE

If the browser does not prompt for a certificate at all, your CAC may not be seated properly in the reader, or the CAC reader drivers may not be installed. Remove and reinsert your CAC. If the problem persists, contact your S6.

CAUTION

Do not allow the browser to save your PIN. Do not use "Remember Me" or autofill options for your MSS login. MSS sessions may contain sensitive operational information.

CAUTION

Do not use a personal device (personal laptop, phone, tablet) to access MSS unless you have received specific written authorization from your unit security officer. Accessing MSS from an unauthorized device is a security violation regardless of whether you successfully log in.

CHAPTER 3 — NAVIGATING THE PLATFORM

BLUF: Once you are logged in, you need to find your unit's applications and data. This chapter covers how to use search, how to navigate the file browser (Compass), and how to recognize the different types of resources in MSS.

3-1. TYPES OF RESOURCES IN MSS

Everything in MSS is a resource. Resources are organized into folders called Projects. Before you can navigate efficiently, you need to know what kind of thing you are looking at.

Table 3-1. MSS Resource Types

Icon	Resource Type	What It Is	What You Do With It
Application window icon	Workshop Application	A built dashboard, form, or report	Open it and use it — dashboards, filters, forms
Table/grid icon	Dataset	A structured table of data (rows and columns)	View, filter, sort, or analyze in Contour
Folder icon	Project	A container for related resources	Navigate into it to find datasets and applications
Globe/sphere icon	Ontology Object Type	A category of real-world objects (units, vehicles, Soldiers)	View and explore in Quiver
Analysis icon	Contour Analysis	A saved analysis or chart	Open to see saved analysis
Lock icon	Restricted resource	You do not have access	Contact data steward to request access
Star icon	Starred/pinned item	A resource you have bookmarked	Click to open quickly from home
Clock icon	Scheduled resource	Shows last-updated timestamp	Check for data currency
Warning triangle	Quality alert	Data quality flag is raised	Read alert; do not use until resolved

TASK 3-1: FIND AND SAVE RESOURCES

CONDITIONS: Operator is logged into MSS and needs to locate a specific application, dataset, or project.

STANDARDS: Operator locates a named resource using search OR Compass navigation, opens it, and bookmarks a frequently used resource to the home screen.

EQUIPMENT: Active MSS session, knowledge of resource name or unit project folder path.

PROCEDURE:

Method 1 — Search (fastest):

1. Click the **Search bar** at the top center of the screen.
2. Type the name or partial name of what you are looking for (e.g., "SITREP" or "readiness").
3. MSS displays results as you type. Use the filter options on the left to narrow by type (Application, Dataset, Project).
4. Click the matching result to open it.

> **NOTE**
>
> Search only returns resources you have permission to see. If a resource you know exists does not appear, contact your data steward — do not assume it does not exist.

Method 2 — Compass (file browser):

1. Click the **Compass icon** in the left sidebar.
2. Navigate the folder tree by clicking folder names to expand them. Folders are organized by organization and project.
3. Find your unit's project folder (typically named for your unit or mission area).
4. Click a resource to open it. Identify resource types by their icons (see Table 3-1).

> **NOTE**
>
> You will only see folders and resources your account has been granted access to. Folders you cannot access appear locked or do not appear at all — this is by design.

Bookmarking a resource:

1. Navigate to the resource you want to bookmark (using either method above).
2. Click the **Star icon** next to the resource name. The star fills in to confirm it is bookmarked.
3. Return to the home screen (click MSS logo, upper left). The resource now appears under Starred/Pinned items.

4. To remove a bookmark, click the star again to toggle it off.

> **NOTE**
>
> Bookmarks are personal — they affect only your view and do not change access for anyone else.

EXAMPLE: SPC Caldwell in the 1st ABCT S4 shop needs the equipment readiness dashboard. She types "readiness" in the search bar, filters to "Application," and finds "1ABCT Equipment Readiness Dashboard." She opens it and clicks the star to bookmark it for tomorrow's shift.

CHAPTER 4 — USING WORKSHOP APPLICATIONS

BLUF: Workshop is the main interface most MSS users will see every day. A developer in your unit or on the MSS team has built an application — a dashboard, a form, a report — and published it for your unit to use. You interact with it the same way you use any website: clicking, reading, filtering, and submitting forms. You do not need to understand how it was built.

> **NOTE**
>
> You are using an application that a SL 2 builder created. If an application is missing a feature you need, is broken, or needs modification, do not attempt to edit it yourself. Contact your unit data steward and reference TM-20, Chapter 5 (Building Workshop Applications) as the appropriate level to address the issue.

4-1. WHAT WORKSHOP APPLICATIONS LOOK LIKE

Workshop applications are web pages inside MSS. They are built from widgets — visual components like charts, tables, filters, and buttons. Every application is different because each unit's needs are different. However, the basic building blocks are the same across all applications.

Table 4-1. Common Workshop Widget Types

Widget	What It Looks Like	What You Do With It
Dashboard / Chart	Bar chart, line graph, pie chart, map	Read the title and legend; hover over data points for values
Metric Tile	A large number with a label (e.g., "847 Soldiers Reporting")	Compare to the standard or threshold to assess status
Object Table	A spreadsheet-like grid of rows and columns	Click a column header to sort; click a row to select it
Filter Panel	Dropdown menus, date pickers, checkboxes, toggle switches	Select values to narrow what the dashboard shows
Action Form	Labeled text fields, dropdowns, and a Submit button	Fill in required fields and submit to write data
Action Button	A button labeled with its function ("Submit SITREP," "Mark Ready")	Click to execute an action against a selected record

Widget	What It Looks Like	What You Do With It
Map Widget	A geographic display with colored icons or layers	Click icons on the map to see record details
Status Badge	A colored dot or label (green, yellow, red)	Check the legend — colors mean different things in different apps
Navigation Tabs	Tabs at the top or a sidebar with page names	Click to switch between pages of the application
Search Box	A text input field inside the application	Type to filter records displayed in the application

TASK 4-1: ORIENT TO A COMMAND-LEVEL APPLICATION

CONDITIONS: Operator is logged into MSS and has been granted access to a command-level Workshop application — typically a commander's update brief (CUB), situation assessment (CUA), or geospatial situational awareness application — and needs to navigate and extract information from it.

STANDARDS: Operator independently opens a command-level application and, without assistance: (1) navigates to the correct page when given a named operational domain (e.g., "personnel readiness" or "equipment status"); (2) reads and correctly states the data currency timestamp from the application header or map widget; (3) clicks a specified map object and correctly reads back the object's unit designation, status, and last-update time from the pop-up panel; (4) uses the map legend to correctly identify what a specified color or icon represents before making any status determination.

EQUIPMENT: Active MSS session, access to a command-level Workshop application, familiarity with Task 4-2 (Read a Dashboard).

PROCEDURE:

Step 1 — Navigate to the command-level application:

1. Use Search or Compass (Chapter 3, Task 3-1) to locate the application by name.
2. If you do not know the application name, ask your unit data steward or section chief — they can provide the correct name and confirm your access.
3. Click the application name to open it.
4. Wait for all widgets and map layers to fully load before interacting.

NOTE — USAREUR-AF Example: Within USAREUR-AF, command-level applications include the Commander's Update Brief (CUB) and Commander's Update Assessment (CUA), which serve as the primary operational picture applications for command staff. Other commands and organizations will have

equivalent applications that serve the same function under different names. The navigation skills in this task apply universally to any Workshop-based command application.

Step 2 — Orient to the application layout:

1. Read the application title and any introductory text visible on the landing page.
2. Identify the navigation structure: tabs across the top, a sidebar, or button-driven navigation.
3. Click through each page tab or navigation element to understand the full scope of the application before acting on any data.
4. Note which page covers which operational domain (e.g., personnel, equipment, operations, logistics).

Step 3 — Read annotated map layers:

Many command-level applications include a map widget displaying geospatial data.

1. Identify the basemap and the data layer overlaid on it. Map markers, icons, and colored polygons represent different object types (units, equipment, events, facilities).
2. Look for a map legend. It is typically accessible via a legend button or icon on the map widget. The legend defines what each color, icon, or shape represents.
3. Read the legend before interpreting any map content. Color coding varies by application — do not assume green means ready without confirming the legend.
4. If the map has multiple layers, a layer control panel (typically in the upper right or left corner of the map widget) lets you toggle layers on and off. Use it to reduce visual clutter when multiple overlapping layers are displayed.

> **NOTE**
>
> Gaia is the MSS map-based geospatial application used across the enterprise for situational awareness and operational overlay display. The skills in this task — reading layers, clicking on map objects, extracting data from pop-up panels — apply to Gaia and any other map-based Workshop application in your environment.

Step 4 — Click on map objects to reveal supporting data:

1. Click any map marker, icon, or polygon. A pop-up panel or side panel will appear displaying the properties of that object.
2. Read the pop-up to identify the object's status, unit, last update time, and any other operationally relevant fields.
3. Some applications allow you to drill down from the map selection into a detail page. If a "View Details" button or similar link appears in the pop-up, click it to see the full record.
4. If clicking a map object does not produce a pop-up, the map may be in a non-interactive display mode, or you may need to select an object type layer first. Check the layer control panel.

Step 5 — Extract and use the information:

1. Identify the data you need for your task (e.g., the readiness status of a specific unit, the location of a facility, the number of events in an area).
2. Note the data currency — look for a "Data as of:" timestamp in the application header or on the map widget. Command applications display real-time or near-real-time data, but the update frequency varies by application.
3. If the information you need is not visible, check whether a filter or page selection is needed first. Some map applications require you to select a filter (unit, date range, category) before all layers are displayed.

CAUTION

Command-level applications may display sensitive operational information about unit positions, readiness, and activities. Handle and protect this information according to its classification level. Do not screenshot, export, or share this data outside of approved channels.

NOTE

If a command-level application is missing information you expect to see, or if the data appears incorrect, do not attempt to interpret or correct it yourself. Report the issue to your unit data steward per Table 1-2 (paragraph 1-7).

TASK 4-2: READ A DASHBOARD

CONDITIONS: Operator is logged into MSS and has access to a Workshop application containing a dashboard view.

STANDARDS: Operator locates and opens a Workshop application, waits for all widgets to load, correctly reads metric tiles, interprets chart axes and legends, understands status color coding, and identifies the data timestamp.

EQUIPMENT: Active MSS session, Viewer access to target application.

PROCEDURE:

1. Locate the application using search or Compass (Chapter 3, Task 3-1).
2. Click the application name. Wait for all widgets to load — loading spinners disappear when complete. Do not interact while loading.
3. Orient yourself: read the title, identify page tabs or sidebar navigation, and note the application's overall structure.

4. **Read the title and context.** The application header and each chart title tell you what you are looking at. Read these before interpreting any numbers.
5. **Read metric tiles first.** Large single numbers (KPI tiles) show the most important summary figures. Examples: "94% — Units Reporting" or "6 — Equipment Deadlines." These give you the overall picture before you dig into charts.
6. **Read charts with the legend open.** Every chart has a title, axis labels, and a legend (a key showing what colors or shapes mean). Read all three before interpreting the chart.
7. X-axis (horizontal) typically shows time, unit names, or categories.
8. Y-axis (vertical) typically shows count, percentage, or quantity.
9. Bars, lines, and pie slices are color-coded. Check the legend.
10. **Read status badges using the legend.** Green/yellow/red colors are common, but their thresholds differ by application. Find the legend or ask your data steward what the thresholds mean for that specific dashboard.
11. **Check the data timestamp.** Look for "Data as of:" or "Last Updated:" text in the application header, footer, or in the metadata panel of individual charts. If the timestamp is older than expected, contact your data steward before making operational decisions based on the data.

NOTE

Workshop applications are read-only by default unless they include a form or an action button. If you can see data but see no Submit buttons or Action buttons, you are in a view-only mode — this is normal and correct for many users.

NOTE

If a Workshop application shows an "Edit" or "Builder" mode option, do not enter it unless you are a designated builder for that application. Entering builder mode and making changes to the application layout can break it for all users. Report any accidental edits to your data steward immediately.

NOTE

Dashboard data reflects the last time the underlying data pipeline ran — it is not necessarily real-time. Know your pipeline's update frequency. Ask your data steward if you are unsure how current the data is.

EXAMPLE: CPL Davis is on the 3rd Infantry Division G4 readiness desk in Wiesbaden. She opens the division readiness dashboard. She reads the metric tile showing "78% — Fully Mission Capable" and then looks at the bar chart showing FMC by brigade. She checks the "Data as of: 101800Z MAR 26" timestamp in the footer. The data is from yesterday's run — current enough for the morning update.

Navigating multi-page applications:

Applications with multiple pages use tabs across the top, a sidebar with page names, or labeled navigation buttons. Read the page labels before clicking to understand the purpose of each section. If a page requires selecting a record first (e.g., select a unit on the Overview page before viewing its Detail page), make that selection before navigating. Use the breadcrumb trail (if visible) to track your location.

TASK 4-3: APPLY FILTERS TO A DASHBOARD

CONDITIONS: Operator has a dashboard open that includes filter controls and needs to narrow the displayed data to a specific unit, date range, or status.

STANDARDS: Operator applies one or more filters, confirms the dashboard updates to reflect the filtered data, and clears filters when done.

EQUIPMENT: Active MSS session, Workshop application with filter controls open.

PROCEDURE:

1. Locate the filter panel. It is typically on the left side or top of the dashboard. Common filter types:
2. **Dropdown menu** — click to open, select one or more values from a list.
3. **Date picker** — click to open a calendar; select start date then end date.
4. **Search box** — type a value to filter a specific field.
5. **Toggle/checkbox** — click to include or exclude a category.
6. Select the filter value you want. For example: in a unit dropdown, select your brigade — "3d BCT, 1st Cavalry Division."
7. The dashboard updates automatically. Charts, tables, and metric tiles now show data only for your selected filter.
8. Apply additional filters as needed. Multiple filters work together — each one narrows the results further.
9. To clear one filter: click the "X" next to the filter value, or select "All" from a dropdown.
10. To clear all filters at once: look for a "Reset Filters," "Clear All," or "X" button, usually near the filter panel header.

NOTE

Filters only affect what you see in your current session. They do not change the underlying data and do not affect what other users see. If you close the application and reopen it, filters reset to default.

EXAMPLE: SSG Torres is reviewing the training completion dashboard for his battalion in Grafenwoehr. He filters the Unit dropdown to "1-7 CAV" and the Training Type to "Weapon Qualification." The dashboard now shows only 1-7 CAV's weapon qualification data. He confirms his battalion's qualification

rate is 91%, which is above the brigade standard of 85%.

TASK 4-4: SUBMIT DATA USING AN ACTION FORM

CONDITIONS: Operator has a Workshop application open that includes a data entry form and is authorized to submit data through that form.

STANDARDS: Operator completes all required fields with accurate information and receives a success confirmation after submitting.

EQUIPMENT: Active MSS session, Workshop application with an Action Form widget, authorization to submit data.

PROCEDURE:

1. Locate the form within the application. Forms contain labeled input fields (text boxes, dropdowns, date pickers, number fields) and a Submit or Confirm button.
2. Identify required fields — they are typically marked with an asterisk (*) or highlighted in some way. The form will not submit until all required fields are completed.
3. Read each field label carefully before entering data. Enter the correct information for each field.
4. **Text fields:** type the required text. Watch field length limits.
5. **Dropdown fields:** click the dropdown and select the correct value from the list. Do not type a value not on the list.
6. **Date fields:** use the date picker — click the field to open the calendar and select the date. Do not manually type dates unless instructed.
7. **Number fields:** type the number only. No commas or special characters unless the field specifies.
8. Review all entries before submitting. Read each field one more time.
9. Click the **Submit** (or **Confirm**) button.
10. Wait for the confirmation message. A green success message means the record was saved. A red error message identifies what went wrong.
11. If submission fails: read the error message, correct the identified field, and click Submit again.

CAUTION

Data submitted through a form writes directly to live operational records. Verify all information before submitting. A SITREP submitted with incorrect data or the wrong unit will require a data steward to manually correct. That takes time and creates confusion.

WARNING

Do not submit data on behalf of another Soldier using your credentials unless you are specifically authorized and directed to do so in your unit SOP. All submissions are logged with your user identity. Submitting records under your credentials that belong to another Soldier is a records integrity violation.

EXAMPLE: PFC Rodriguez is the readiness NCO for HHC, 2nd BCT in Vilseck. He submits the daily SITREP through the unit's Workshop SITREP application. He selects his unit from the dropdown, enters the readiness numbers for each status category, adds a remarks note, and clicks Submit. The green confirmation message "SITREP submitted successfully — 111845Z MAR 26" appears. He screenshots the confirmation for his records.

NOTE

The action form you are submitting was configured by a SL 2 builder using the Ontology Manager. If an action is missing, not functioning correctly, or needs a new field, this is a SL 2 or SL 3 builder task. Report the issue to your data steward. Refer to TM-20, Chapter 4-2 (Ontology Manager Interface Overview) for builder-level action configuration. Complex multi-step action workflows are SL 3 level — refer to TM-30, Chapter 4, Section 4-4 (Action Design).

TASK 4-5: EXECUTE AN ACTION BUTTON

CONDITIONS: Operator has a Workshop application open that includes an action button (e.g., "Mark Complete," "Approve," "Close Report") and is authorized to execute that action.

STANDARDS: Operator reads the action label and confirmation dialog, understands what the action will change, and successfully executes the action or deliberately cancels it.

EQUIPMENT: Active MSS session, Workshop application with action button, authorization to execute the action.

PROCEDURE:

1. Locate the action button. Action buttons are labeled with their function: "Update Status," "Submit SITREP," "Mark Ready," "Approve," "Close."
2. If a record must be selected before the action applies (e.g., click a row in a table to select a unit, then click "Update Status"), make that selection first.
3. Before clicking: read the button label and any surrounding text to understand exactly what the action will do and to what record.
4. Click the action button.

5. A **confirmation dialog** appears. It describes the action and its effect (e.g., "This will mark Unit 3-69 AR as Fully Mission Capable as of 111900Z MAR 26. This cannot be undone. Confirm?"). Read it completely.
6. Click **Confirm** to execute the action, or **Cancel** to abort without making any change.
7. Wait for the success or error message.
8. Verify the result: check that the relevant record, status indicator, or table row updated as expected.

CAUTION

Actions change live operational data. Some actions cannot be undone — the confirmation dialog will tell you if this is the case. If you are not sure what an action does, click Cancel and ask your supervisor or data steward before proceeding.

EXAMPLE: 1LT Chen is a readiness officer in the 173rd Airborne Brigade in Vicenza. She selects a vehicle record from the maintenance status table and clicks "Mark FMC." The confirmation dialog reads: "Mark M1278 HMMWV (Bumper Number 3A-017) as Fully Mission Capable? This action will update the equipment record and notify the S4. Confirm?" She verifies the bumper number matches the vehicle, then clicks Confirm.

TASK 4-6: EXPORT DATA FROM A WORKSHOP APPLICATION

CONDITIONS: Operator has a Workshop application open with export functionality enabled, is authorized to export that data, and has an approved destination for the exported file.

STANDARDS: Operator verifies export authorization, selects correct format, downloads the file, and handles it IAW the data's classification level.

EQUIPMENT: Active MSS session, Workshop application with export button, authorized storage destination.

PROCEDURE:

1. Locate the export button. It is typically labeled "Export," "Download," or shown as a downward arrow icon. It may be in the application toolbar or in a table header.
2. **Before clicking:** verify two things —
3. You are authorized to export this data (check with your data steward if unsure).
4. Your destination (laptop hard drive, shared drive, USB) is approved for the data's classification level.
5. Click the export button.
6. If prompted, select the file format. CSV is a plain spreadsheet format; Excel (.xlsx) is a formatted spreadsheet. Select based on what you need.

7. The file downloads to your browser's default download folder.
8. Move the file immediately to its intended authorized location.
9. Handle the file IAW the data marking on it. If the data is CUI, treat the file as CUI. If it is SECRET, treat it as SECRET.

WARNING

Exported data retains its classification and handling requirements outside of MSS. A CSV file of SECRET data is a SECRET document. Placing that file on an unclassified shared drive, emailing it unencrypted, or leaving it on a personal device are all security violations. If you are uncertain whether an export is authorized or where the file should go, do not export. Contact your data steward first.

NOTE

Not all Workshop applications have an export button. If there is no export button, exporting that data is not authorized for that application. Do not use screen capture, copy-paste into a spreadsheet, or any other workaround to extract the data.

4-8. AIP AND AI-ASSISTED FEATURES IN WORKSHOP APPLICATIONS

BLUF: MSS includes AI-assisted tools under the AI Platform (AIP). These tools are embedded in Workshop applications — operators encounter them as alerts, recommendations, and chat interfaces within applications their unit uses. They can help you find information, summarize data, and draft text faster. They are useful — and they require human judgment before any AI output is used operationally. The AI does not have rank. You do.

AIP (AI Platform) is the AI layer of MSS. It connects large language models (LLMs) — AI systems trained to understand and generate natural language — to your unit's data in MSS. This allows you to ask questions in plain English and receive summaries, analyses, and recommendations.

Think of an AIP agent as a very capable staff assistant that can quickly search through thousands of records and give you a summary. That assistant can be wrong. Your job is to check their work before briefing the commander.

In USAREUR-AF, AIP tools are authorized for: - Summarizing readiness data across units - Drafting SITREP text based on structured data inputs - Answering questions about data in MSS using natural language - Surfacing patterns or anomalies in operational data

AIP tools are NOT authorized for: - Making final operational decisions — a human officer, NCO, or official must make every decision - Generating official orders, directives, or legal documents without human review and signature - Accessing data above your clearance level — access controls apply to AI

just as they apply to you - Connecting to external systems, websites, or the public internet — AIP operates within the MSS boundary only

WARNING

AI-generated content in MSS is NOT authoritative and is NOT always correct. AI tools can produce outputs that sound plausible but are factually wrong. This is called "hallucination" — the AI generates confident-sounding text that is not supported by the actual data. All AI outputs must be reviewed by a qualified human before being used to make operational decisions, submit reports, or brief commanders. The human operator is responsible for the accuracy of any AI-assisted product. If you brief a commander on AI output that you did not verify, and it is wrong, that is on you — not the AI.

Table 4-2. AIP Capabilities and Limits

AI tools CAN do this	AI tools CANNOT do this
Summarize data from MSS datasets you are authorized to see	Access data above your clearance level
Answer questions in natural language	Make binding operational decisions
Draft text summaries and SITREP language	Guarantee accuracy — always verify
Flag anomalies and trigger alerts	Modify data (agents are read-only; only Actions write data)
Navigate between related records	Access external websites or systems
Maintain context within a conversation	Override classification markings

TASK 4-8A: READ AND RESPOND TO AN AIP LOGIC ALERT

CONDITIONS: Operator has access to a Workshop application that includes an AIP Logic workflow — an automated process that surfaces alerts, recommendations, or status changes.

STANDARDS: Operator reads the workflow output, identifies the underlying data it acted on, verifies that data, and applies judgment before taking action based on the workflow output.

EQUIPMENT: Active MSS session, Workshop application with AIP Logic workflow.

NOTE

AIP Logic workflows are designed and configured by SL 3 advanced builders. You are using a workflow that has been built for you. If the workflow produces unexpected outputs, follow the human review steps in this task. If the workflow itself is broken or needs modification, report to your data steward — do not attempt to reconfigure it. For SL 3 builder reference, see TM-30, Chapter 6 (AIP Logic Configuration).

PROCEDURE:

1. AIP Logic workflows appear in Workshop applications as **automated alerts or recommendations.** They may display as:
2. A highlighted alert box: "Unit 2-8 CAV readiness has dropped below 70% — review recommended."
3. A status change flag: "Maintenance deadline status updated — 3 vehicles flagged."
4. A triggered notification in the notification bell.
5. Read the workflow output carefully. Note what it is telling you and what action (if any) it is recommending.
6. Identify the **underlying data** the workflow acted on. Look for a link or reference to the source record — click through to see the actual data.
7. **Verify the source data** by reviewing it directly. Does the data support the alert? Is the timestamp current?
8. Apply your own judgment: does this alert make sense given what you know about the situation?
9. If the alert is valid and action is required, take the appropriate action (consult your supervisor, execute a Workshop action, escalate to data steward).
10. If the alert appears incorrect or unexpected, do NOT act on it. Report it to your data steward.

NOTE

AIP Logic workflows are automated rules built by your unit's data engineers based on thresholds and business rules. They are not infallible. A workflow that alerts on the wrong condition, fails to alert on a real condition, or produces unexpected outputs should be reported so it can be corrected.

EXAMPLE: SGT Okonkwo is monitoring the readiness dashboard for 1-9 FA in Grafenwoehr. An AIP Logic alert appears: "Personnel readiness below 80% threshold — 14 Soldiers flagged non-deployable." He clicks the alert to see the source records. He reviews the 14 records and confirms 12 are legitimately non-deployable due to medical status. Two appear to be data entry errors — Soldiers who completed medical clearances yesterday but have not been updated. He reports the two errors to the data steward and uses the 12 correct records in his morning report.

TASK 4-8B: INTERACT WITH AN AIP AGENT (CHAT INTERFACE)

CONDITIONS: Operator has access to an AIP Agent embedded in a Workshop application or accessible through Agent Studio, and needs to query operational data using natural language.

STANDARDS: Operator enters a clear, specific query, receives a response, verifies the key facts against source records, and uses the response appropriately after verification.

EQUIPMENT: Active MSS session, AIP Agent interface.

> **NOTE**
>
> AIP Agents are AI interfaces designed for operator use, configured by SL 3 builders. Your role is to interact with the agent and validate its outputs before acting on them. If the agent produces consistently incorrect, outdated, or operationally unsound information, report to your data steward with screenshots or a summary of the issue. Do not alter the agent configuration. See TM-30, Chapter 6 for builder-level AIP configuration.

PROCEDURE:

1. Locate the **Agent chat interface.** It appears as a chat panel within a Workshop application, or as a standalone Agent Studio window. It looks like a messaging app — there is a text input box at the bottom.
2. Think about what you want to know **before** typing. The more specific your question, the better the answer.
3. Instead of: "How are we doing?"
4. Type: "What is the current mission capable rate for wheeled vehicles across 21st TSC as of today?"
5. Type your question in the chat input box and press Enter or click the Send button.
6. The agent queries MSS data and responds in the chat panel. The response may include text summaries, data tables, percentages, or links to source records.
7. **Read the response carefully.** Do not just use the first number you see.
8. **Verify key facts:** click through to any source records the agent references. Confirm the numbers match what you see in the underlying data.
9. If you want to drill deeper, type a follow-up question: "Break that down by brigade." The agent maintains context within a conversation.
10. If the response seems wrong, navigate directly to the data to cross-check. If the discrepancy is significant, report it to your data steward.
11. **Do not copy AI text verbatim into an official document** without verifying the facts. Revise for accuracy and official language before use.

NOTE

AIP Agents only access MSS data you are authorized to see. An agent cannot reach data outside your access level — this is enforced at the data layer, not by the AI. If an agent says it cannot find information, the data may not exist in MSS, the pipeline may not have run, or you may not have access to that data.

NOTE

Do not enter sensitive personal identifying information (SSN, full medical details) into the agent chat interface unless the interface is specifically designated for that data. Chat inputs may be logged for system improvement purposes.

EXAMPLE: WO2 Patterson at 21st TSC G4 in Sembach Kaserne needs a quick readiness summary for the weekly sustainment brief. She opens the AIP Agent in the sustainment dashboard and types: "What percentage of Class IX parts requests from the past 7 days have been filled within the 48-hour standard, broken down by commodity class?" The agent returns a table with fill rates by class. She clicks through to verify two of the numbers against the dataset. Both match. She uses the table in her brief, noting "Source: MSS AIP Agent output, verified against raw data, as of 111900Z MAR 26."

CHAPTER 5 — WORKING WITH DATA

BLUF: Most users will interact with data through Workshop applications. This chapter covers what to do when you need to go deeper — opening datasets directly, using Contour for basic analysis without writing code, and using Quiver to explore linked records. It also covers how to verify that data is current and what to do when something looks wrong.

5-1. DATA BASICS — WHAT DATA IN MSS LOOKS LIKE

Data in MSS is organized into **datasets** — structured tables with rows and columns, the same concept as a spreadsheet. Each column has a name (the field name) and a data type (text, number, date, yes/no). Each row is one record — one Soldier, one vehicle, one SITREP submission, one event.

Data in MSS flows through processing layers before you see it:

```
Army source systems (GCSS-A, DCPDS, MEDPROS, unit feeds)
        ↓
Ingestion and cleaning (data engineers process the raw data)
        ↓
Datasets in MSS (what you see in Compass)
        ↓
Workshop applications (dashboards and forms built on top of datasets)
```

You interact with the cleaned, curated layer. You will not see raw, unprocessed data in operational applications.

TASK 5-1: VIEW AND READ A DATASET

CONDITIONS: Operator has located a dataset in MSS using search or Compass and has Viewer access to it.

STANDARDS: Operator opens the dataset, correctly identifies column names, data types, row count, and last-updated timestamp within 5 minutes.

EQUIPMENT: Active MSS session, Viewer access to target dataset.

PROCEDURE:

1. Click the dataset name in search results or Compass to open it.

2. The dataset opens in a preview view — a table showing the first 100 rows of data.
3. Read the **column headers** across the top row. Each header is the name of a field.
4. Look at the **data type indicator** under each column header. Common types:
5. **Text (string):** words, names, codes — displayed as letters.
6. **Number (integer or decimal):** quantities, counts, percentages.
7. **Date/Timestamp:** dates and times (often shown in ISO format: 2026-03-11T18:30:00Z).
8. **Boolean (true/false):** yes/no, active/inactive fields.
9. Read several rows to understand the range of values in each column.
10. To **sort** by a column: click the column header. Click again to reverse the order.
11. To **filter** rows: use the filter bar above the preview table. Select a column and enter a filter value.
12. Open the **metadata panel** (look for an "Info," "Details," or "Properties" tab, usually on the right side). Record the:
13. Total row count
14. Last updated timestamp
15. Schema (full list of all columns and their types)

CAUTION

You are viewing a live preview of the dataset. Do not attempt to edit data directly in the preview. The preview is read-only. If you need to correct data, use the designated Workshop application form for that data type, or contact your data steward.

TASK 5-2: PERFORM A BASIC LOOKUP IN CONTOUR

CONDITIONS: Operator has Viewer access to a dataset and access to Contour, and needs to answer a specific question about the data (e.g., "How many vehicles are in RED status?").

STANDARDS: Operator opens Contour with a target dataset, sorts and filters to find the answer, and reads the result correctly.

EQUIPMENT: Active MSS session, Viewer access to target dataset, Contour access.

PROCEDURE:

1. Open the target dataset in Compass.
2. Click the **Analyze in Contour** button in the top toolbar. Contour opens with the dataset loaded.
3. The dataset appears as a table in the Contour workspace — rows and columns, similar to a spreadsheet.

4. To **sort** by a column: click the column header in the Contour table. Click again to reverse.
5. To **filter** to specific records: click **Add Filter**, select a column, and enter the value you want (e.g., filter "status" to "RED").
6. Read the filtered result. The row count at the bottom of the table tells you how many records match.
7. To clear a filter, click the "X" on the filter tag.

NOTE

Contour is a read-only analysis tool — it does not modify the underlying dataset. For more advanced Contour analysis (aggregations, charts, saved analyses), see SL 2.

CAUTION

Before sharing any Contour output, verify that the combined output does not reveal information at a higher classification than what you are authorized to share (see Aggregation Risk, Section 6-4).

EXAMPLE: SSG Kim at V Corps G4 needs to know how many Class IX parts requests are overdue. She opens the parts request dataset in Contour, filters "status" to "OVERDUE," and reads the row count: 47 overdue requests. She notes the result for her morning report.

TASK 5-3: LOOK UP AN OBJECT IN QUIVER

CONDITIONS: Operator has access to Quiver and needs to find information about a specific entity (a unit, vehicle, Soldier, or other tracked object).

STANDARDS: Operator opens Quiver, selects the correct object type, locates a specific object, and reads its properties.

EQUIPMENT: Active MSS session, Quiver access, access to target object types.

PROCEDURE:

1. Navigate to **Quiver** from the left sidebar or application menu.
2. The **Object Type catalog** appears on the left. Select the type you want to explore (e.g., "Vehicle," "Unit," "SoldierReadiness").
3. The **object list** loads in the center panel, showing all objects of that type you are authorized to see.
4. To find a specific object, use the **filter panel**: click "Add Filter," select a property (e.g., "unit"), and enter the value (e.g., "1-7 CAV").
5. Click any object in the list to open its **detail panel** on the right. Read the properties displayed.

NOTE

Quiver shows data from the Ontology — the semantic layer of MSS that organizes data as real-world entities and their relationships. Objects in Quiver are the same records that power Workshop applications. For advanced Ontology exploration (link traversal, related objects, Object Type relationships), see SL 2.

NOTE

Quiver is read-only for consumer users. You cannot edit properties or create objects from Quiver.

EXAMPLE: SFC Adams at 21st TSC needs to verify the assigned unit for a specific vehicle. He opens Quiver, selects the "Vehicle" object type, filters by bumper number, and reads the "Assigned Unit" property in the detail panel.

TASK 5-4: VERIFY DATA CURRENCY AND SOURCE

CONDITIONS: Operator has a dataset or Workshop application open and needs to confirm that the data is current enough for its intended use (e.g., morning briefing, operational decision, report submission).

STANDARDS: Operator locates the last-updated timestamp, determines whether the data meets the currency requirement for the intended use, and takes appropriate action if the data is stale.

EQUIPMENT: Active MSS session.

PROCEDURE:

1. **For a dataset:** open the metadata or info panel (look for an "Info" or "Details" tab). Find the **Last Updated** timestamp.
2. **For a Workshop application:** look for a data timestamp in the application header, footer, or chart tooltips. It may say "Data as of: [date/time]" or "Last refreshed: [date/time]."
3. Compare the timestamp to your **currency requirement:**
4. For readiness reporting: data older than 24 hours typically requires verification with the source unit before operational use.
5. For real-time operational tracking: data older than the pipeline update interval (ask your data steward) is stale.
6. For historical analysis or trend review: older data may be acceptable — confirm with your supervisor.
7. If the data appears to be **outside the expected update interval** (e.g., the pipeline normally runs hourly but the data is 6 hours old):
8. Do not assume the data is correct.

9. Note the timestamp.
10. Contact your data steward and report it: "The [dataset/application name] shows data as of [timestamp]. Expected update interval is [X]. This may indicate a pipeline failure."
11. If you are unsure what the expected update interval is, ask your data steward.

Table 5-1. Data Currency Decision Guide

Data timestamp vs. expected interval	Meaning	Action
At or near expected interval	Data is current	Use normally
Moderately past expected interval (up to 2x interval)	Possible pipeline delay	Note it; use with caution; notify data steward
Significantly past expected interval (more than 2x)	Pipeline likely failed	Do not use for operational decisions; report to data steward
"No data available" message	Feed is down or empty	Report to data steward; do not treat as zero
Warning triangle on dataset	Quality flag raised	Read the alert; do not use until resolved

TASK 5-5: HANDLE STALE OR CONFLICTING DATA

CONDITIONS: Operator observes data in MSS that appears outdated (timestamp is more than 4 hours old for a daily-refresh dataset, or more than the expected refresh interval) OR data in MSS conflicts with information reported through other channels (e.g., unit reports 75% readiness but MSS shows 40%).

STANDARDS: Operator correctly identifies the data currency issue, takes appropriate action without altering data, and escalates within 30 minutes if the discrepancy is operationally significant.

EQUIPMENT: Active MSS session. Access to the dashboard or dataset in question.

PROCEDURE:

1. Check the data timestamp. On most dashboards, look for "Data as of: [date/time]" in the footer or header. In a dataset view, check the "Last Updated" column.
2. Compare the timestamp to the expected refresh schedule. If the data is older than the scheduled refresh interval, the pipeline may have failed.
3. If data appears stale: do NOT assume the data is correct. Note it as potentially unreliable.
4. If data conflicts with information from another source: do NOT use MSS data as authoritative until the discrepancy is resolved. Note both values and the source of each.
5. Contact your unit data steward. Provide: (a) the name of the dashboard or dataset, (b) the current timestamp shown, (c) what the data shows vs. what you expected or heard from another source.

6. The data steward will investigate the pipeline and confirm or correct the data.
7. For time-critical operations where the discrepancy cannot wait for pipeline resolution: brief your commander on the data uncertainty. Do not present unverified MSS data as confirmed.

NOTE

A data discrepancy is not automatically an error — source system delays, network issues, or reporting lag are common. The standard response is to flag it and escalate, not to ignore it or work around it.

5-2. WHAT TO DO WHEN DATA LOOKS WRONG

If you see data that appears incorrect — wrong unit, wrong number, a value that does not match what you know to be true:

1. **Do not correct it yourself** unless you are using an authorized Action or form specifically designed for that purpose.
2. **Note the specifics:** dataset name, row identifier (which record), field name, incorrect value, and what you expected the value to be.
3. **Do not share or act on the incorrect data** operationally — treat it as suspect.
4. **Contact your unit data steward** with the specifics. The data steward will trace the error to its source and coordinate the correction.

CAUTION

Guessing at corrections, editing records outside of authorized interfaces, or working around incorrect data without reporting it degrades data integrity for everyone who uses that data downstream. One bad record can cascade into multiple bad reports.

NOTE

Distinguish between data that looks wrong due to user error (operator-fixable) and systematic data quality problems (builder/engineer responsibility). Operator-fixable: wrong filter applied, stale view (refresh), user-level permissions issue. Escalate to data steward → SL 2 builder: pipeline configuration error, incorrect transform logic, broken data feed from a known source. Escalate to data steward → SL 3 advanced builder or SL 4 developer: systematic data corruption, incorrect schema mapping, validation failures at ingestion. Do not attempt to modify pipelines or datasets yourself. Refer to TM-30, Chapter 3 (Advanced Pipeline Builder) for builder-level pipeline diagnostic context.

5-5. UNDERSTANDING VAULTIS-A — THE DATA QUALITY STANDARD

Every MSS data product is measured against eight quality dimensions known as **VAULTIS-A** (DDOF Playbook v2.2, December 2025). As a data consumer, you do not score products yourself, but you should understand what these dimensions mean so you can evaluate whether the data you are using is trustworthy.

Dimension	What It Means for You
V — Visible	Can you find this data in the catalog without someone telling you where it is?
A — Accessible	Can you actually open and use it with your current access?
U — Understandable	Do field names, column headers, and descriptions make sense? Is there a user guide?
L — Linked	Can you trace where this data came from and what feeds into it?
T — Trusted	Has someone verified this data is accurate? Is there a refresh schedule?
I — Interoperable	Can this data be shared with other systems or Allied partners?
S — Secure	Are the classification markings correct? Are access controls enforced?
A — Auditable	Can you prove who accessed this data and when?

What to look for: If a data product in MSS shows a quality score or certification badge, it means the product has been evaluated against VAULTIS-A. Products scoring 85% or higher across all eight dimensions have passed the DDOF Phase 3 quality gate and are approved for operational use. Products below that threshold may have documented limitations.

Your role as a consumer: Report any quality issues to your data steward. If data looks stale, incomplete, or inconsistent, that information helps the product owner maintain the VAULTIS-A score. You are the front-line quality sensor.

CHAPTER 6 — SECURITY, CLASSIFICATION, AND MARKINGS

BLUF: MSS enforces data security through markings — labels on data that restrict who can see it and what they can do with it. This chapter explains how to read those markings, what you are and are not authorized to do with marked data, and what to do when something goes wrong.

6-1. WHAT MARKINGS ARE AND HOW THEY APPEAR

Markings in MSS are labels applied to datasets, applications, and individual objects. They control who can see the data. Markings appear as colored badges or text labels near the resource name — in the file browser (Compass), in application headers, and in dataset metadata.

Table 6-1. Common Markings in MSS

Marking	Meaning	What It Means for You
UNCLASSIFIED	No national security classification	You can still have handling restrictions — check for other markings
CUI	Controlled Unclassified Information	Requires protection — cannot be placed on public-facing systems or sent unencrypted
FOUO (legacy)	For Official Use Only	Retired marking — now handled under CUI. Same protection requirements apply.
SECRET	National Security classification	Requires SECRET clearance to access; must be handled on approved systems
[AOR Label]	Data limited to a specific Area of Responsibility	You must have the AOR marking assigned to your account
[Role Label]	Data limited to a specific function (e.g., S2-only, Medical)	Your role must match the marking to access the data

NOTE

In MSS, markings are applied to **data**, not just documents. A dataset marked SECRET means every row in that dataset is SECRET level. If you can see the data in MSS, your assigned markings authorize you to see it. If you accidentally see data at a level you are not cleared for, follow the procedure in Task 6-2 immediately.

TASK 6-1: VERIFY YOUR OWN MARKINGS AND ACCESS LEVEL

CONDITIONS: Operator is logged into MSS and wants to confirm what data access and markings are assigned to their account.

STANDARDS: Operator locates the profile page, identifies all assigned markings, and understands what each marking grants access to.

EQUIPMENT: Active MSS session.

PROCEDURE:

1. Click your **Profile icon** in the upper right corner.
2. Select **Profile** or **Account Settings** from the dropdown.
3. In your profile, locate the **Markings** or **Access** section. This lists all markings currently assigned to your account.
4. Compare your markings to the data you need to access. If a required marking is not listed, contact your data steward to request it through proper channels.
5. Review your **project access list** — the projects and folders your account can see.
6. If you have access to projects or data no longer relevant to your current assignment (e.g., after a PCS or role change), notify your data steward to remove that access. Keeping unnecessary access is a security risk, not a convenience.

NOTE

You cannot grant yourself markings or expand your own access. All marking changes must go through your supervisor and the MSS administration team via your data steward.

TASK 6-2: RESPOND TO MISROUTED OR HIGHER-THAN-AUTHORIZED DATA

CONDITIONS: Operator navigates to data in MSS that appears to be at a classification level above their clearance, or that carries markings they are not authorized for.

STANDARDS: Operator immediately stops, closes the page, does not interact with the data, and reports the incident within one hour.

EQUIPMENT: Active MSS session (being exited).

PROCEDURE:

1. **STOP. Do not read the data.** If you realize the data may be above your clearance, stop reading immediately — do not scroll, do not continue reading to confirm.
2. **Do not screenshot, copy, save, or otherwise capture the data.**
3. **Do not discuss the content** of what you saw with coworkers.
4. **Close the browser tab** immediately. Navigate away from the page.
5. **Write down** (on paper is fine): the URL or resource name you accessed, the approximate time, how you got there (search? link from another page?), and that you stopped reading as soon as you realized the issue.
6. **Report to your supervisor and unit security officer within one hour.** Provide the written record you made in step 5.
7. **Follow your unit's security incident reporting SOP.** Your security officer will determine whether a formal report is required and what remediation steps to take.

WARNING

This is a potential security incident. Report it immediately, regardless of whether you believe the data was accessible in error or whether you think you actually read anything sensitive. The security officer makes that determination — not you. Failing to report is itself a security violation and can result in adverse action.

6-2. AUTHORIZED VS. NOT AUTHORIZED — QUICK REFERENCE

Table 6-2. Authorization Boundaries for MSS Users

Action	AUTHORIZED	NOT AUTHORIZED
Viewing data	Only at your clearance level and markings	Any data above your clearance or markings
Filtering and sorting in dashboards	Yes, in all applications you have access to	Editing or modifying data outside authorized forms
Submitting forms	Yes, in authorized applications	Submitting under another Soldier's identity without authorization
Executing action buttons	Yes, in authorized applications	Executing actions you have not been briefed on or trained for
Exporting data	Yes, with authorization, to approved locations	Exporting to unapproved systems or devices
Sharing MSS links	Yes, with users who have authorized access	With users who do not have authorization
Screenshots of dashboards	Only UNCLASSIFIED or where approved	Screenshots of classified data on an unclassified device
Using AIP agents to query data	Yes, for authorized data	Inputting classified data into unauthorized AI tools
Using AI output in official products	Yes, after human verification	Verbatim AI output in official reports without verification
Correcting data	Only through authorized forms and Actions	Manual editing outside of designated interfaces

6-3. HANDLING EXPORTS, SCREENSHOTS, AND SHARED CONTENT

Data does not become less sensitive just because you moved it out of MSS. When you export, screenshot, print, or share MSS content, that content inherits the classification of the data it contains.

Exports: - Only export through the authorized Export button in Workshop. Do not copy-paste data from the screen into a spreadsheet. - Move exported files immediately to an approved storage location. - Mark exported files IAW the data's classification (e.g., add "CUI" to the filename or document header). - Do not email exported files in unencrypted form if the data is CUI or above.

Screenshots: - Screenshots of UNCLASSIFIED data are generally permissible for official use purposes. - Screenshots of CUI data must be handled as CUI. - Screenshots of SECRET or higher data on an unclassified device are a security violation. - When in doubt, ask your security officer before screenshotting.

Printing: - Print MSS output to approved printers only (printers on the approved network for that classification level). - Mark printed documents IAW classification — add classification header and footer manually if the print output does not include them. - Handle printed documents IAW your unit's classified document procedures.

Sharing links: - MSS links work only for users who have authorization to the resource. A link shared with an unauthorized user will result in an "Access Denied" error — this is normal and intentional. - Do not attempt to share data by other means (screenshots, email attachments) if the recipient does not have MSS access. Instead, work with your data steward to ensure the right people have appropriate MSS access.

NOTE

Builders who create data products (pipelines, datasets, Workshop applications) are responsible for ensuring those products carry correct classification markings before publication. If you receive an export or data product with markings that appear incorrect, report it immediately to your data steward before sharing or acting on the data. Refer to TM-20, Chapter 8 (Builder Standards and Governance) for builder-level data marking responsibilities.

6-4. AGGREGATION RISK

CAUTION

Combining multiple pieces of unclassified or lower-classification data can produce a product that is classified at a higher level. This is called **aggregation risk.**

A simple example: A unit's location is UNCLASSIFIED. A unit's personnel strength is UNCLASSIFIED. A unit's equipment status is UNCLASSIFIED. A product that combines all three for a specific unit may be classified SECRET or higher because it reveals that unit's combat capability at a specific place and time.

Before exporting, sharing, or publishing any analysis that combines multiple data elements from MSS: - Ask yourself: does this combined product reveal something more sensitive than each individual element? - When in doubt, have your unit security officer or data steward review the combined product before release. - Do not assume that because each source was UNCLASSIFIED, the combined product is UNCLASSIFIED.

6-5. INCIDENT REPORTING PROCEDURES

Table 6-3. Security Incident Reporting

Incident	Report To	When
Accessed data above your clearance	Supervisor and unit security officer	Within 1 hour
Accidental export to unauthorized location	Supervisor and unit security officer	Immediately
Lost or stolen device containing MSS data	Supervisor, security officer, and S6	Immediately
Suspected compromise of your MSS account	Unit S6 and MSS admin team	Immediately
Another user accessing your account	Supervisor and unit security officer	Immediately
AI output that appears to reveal classified information	Data steward and unit security officer	Immediately

After reporting a security incident, preserve all records (browser history, screenshots if safe to take, written notes) until the security officer tells you to do otherwise.

NOTE

All actions you take in MSS — form submissions, data modifications, and application interactions — are logged with your credentials, timestamp, and action type. These logs are retained for accountability reviews, security audits, and incident investigation. You are personally accountable for all activity associated with your credentials.

CHAPTER 7 — TROUBLESHOOTING AND SUPPORT

BLUF: Most MSS problems are one of a small number of common issues with straightforward fixes. If you cannot solve the problem yourself using this chapter, escalate with the right information. Do not attempt fixes that might affect operational data.

7-1. COMMON PROBLEMS AND SOLUTIONS

Table 7-1. MSS Troubleshooting Guide

Problem	Likely Cause	Operator Action
Browser does not prompt for certificate on login	CAC not seated, reader driver issue, or browser config	Remove and reinsert CAC; restart browser; contact S6 if persists
PIN rejected at login	Incorrect PIN entry or locked CAC	Re-enter PIN carefully; 3 failures locks CAC — contact S6 for unlock
"Account not found" or login fails after correct PIN	Account not provisioned or deactivated	Contact data steward to confirm account status
Logged in but cannot see a project	Account not granted access to that project	Contact data steward to request access — do not attempt workarounds
Dashboard shows "No data"	Filter returns zero results, or pipeline failed	Clear all filters first; if still empty after filter clear, contact data steward
Dashboard data looks outdated	Pipeline has not run recently	Note the timestamp; contact data steward with the timestamp
Application will not load or freezes	Browser or network issue	Refresh the page (F5); try a different browser; contact MSS Help Desk if persists
Form will not submit	Required field empty, or validation error	Read the error message carefully; correct the specific field indicated; resubmit
Action button gives an error	Permissions issue, data conflict, or missing required record selection	Note the full error message; contact data steward
Action or form submitted but data not updated	Pipeline processing delay	Wait 5 minutes; refresh; if still not updated, contact data steward

Problem	Likely Cause	Operator Action
Contour shows unexpected results	Incorrect grouping, filter, or wrong dataset	Review Group By and filter settings; re-read the dataset schema
AIP agent gives an incorrect answer	AI error, or data not yet in MSS	Verify data directly in dataset; report agent error to data steward with screenshot
"Access Denied" on a resource	You do not have permission for that resource	Contact data steward — do not attempt to access through alternate routes
Session expired, kicked back to login	Normal session timeout	Log back in with your CAC — this is expected behavior
Cannot see export button	Export not authorized for that application	Contact data steward — do not use other methods to extract data
Application widget not displaying / action form broken	Workshop configuration error	Contact data steward → SL 2 builder (TM-20, Ch. 5)
Data consistently wrong or missing across all users	Pipeline or transform issue	Contact data steward → SL 3 builder or SL 4 developer (TM-30, Ch. 3)
AIP workflow producing wrong outputs	AIP Logic configuration	Contact data steward → SL 3 builder (TM-30, Ch. 6)
Need new dataset, new Object Type, or new action	Build request	Contact data steward → SL 2 or SL 3 builder depending on complexity

7-2. SECURITY INCIDENT RESPONSE PROCEDURE

If you suspect a security incident — unauthorized data access, mishandled classified information, data visible that should not be, or suspicious activity on your account — take the following steps immediately:

1. **STOP.** Do not continue the current activity.
2. Do not attempt to investigate or fix it yourself.
3. Note the time, what you were doing, and what you observed.
4. Contact your supervisor immediately.
5. Contact the USAREUR-AF C2DAO via your unit's data steward.
6. Do not discuss details over unsecured channels.

WARNING

A security incident is not a troubleshooting problem — it is a command responsibility. Do not delay reporting to investigate on your own. Refer to Chapter 6, Section 6-5 and Task 6-2 for additional incident response procedures.

7-3. REPORTING AI ERRORS AND UNEXPECTED OUTPUTS

If an AIP agent or Logic workflow produces output that is incorrect, unexpected, or potentially harmful:

1. **Do not act on the output.**
2. Take a screenshot of the query you entered and the output you received.
3. Note the application name, the query, and what you expected versus what you got.
4. Report to your unit data steward with the screenshot and description.
5. The data steward will escalate to the MSS team for investigation and correction.

7-4. SELF-HELP VS. ESCALATE — DECISION GUIDE

Handle yourself before escalating: - Re-insert CAC and restart browser for certificate issues - Clear filters and refresh the page for missing data - Re-read field requirements and error messages before a second form submission - Check your bookmarks and search again if you cannot find a resource

Escalate to your unit data steward: - Any data quality or accuracy issue - Missing access to a project or dataset you need for your duties - Pipeline appears to have stopped updating (timestamp significantly stale) - Contour or Quiver producing unexpected results you cannot explain - An action or form submission that did not produce the expected result

Escalate to your unit security officer: - Any data you believe you accessed above your clearance - Suspected account compromise - Security incident of any kind

Escalate to USAREUR-AF MSS Help Desk (through unit S6/G6): - System-level errors with error codes - Application will not load after multiple browser refreshes - Cannot reach the MSS portal at all (may be a network or system outage) - Hardware or CAC reader issues after S6 basic troubleshooting is exhausted

7-5. INFORMATION TO HAVE READY BEFORE YOU CALL FOR HELP

Do not call the Help Desk or data steward empty-handed. Having the right information ready will cut the time to resolution significantly.

Collect the following before making contact:

1. **Your username** — shown in your profile page in MSS.
2. **The name and URL of the application or dataset** — copy the exact text from the browser address bar.
3. **The exact error message** — screenshot it if possible. If you cannot screenshot, write it down word for word, including any error codes.
4. **The time the error occurred** — include time zone.
5. **Steps you took immediately before the error** — "I clicked X, then selected Y, then clicked Z, and got this error."
6. **Is the problem consistent or intermittent?** — Does it happen every time, or only sometimes?
7. **Your browser type and version** — in Chrome: click the three-dot menu → Help → About Google Chrome.

7-6. MSS SUPPORT ESCALATION PATH

Table 7-2. MSS Support Contacts

Issue Type	First Point of Contact	Escalation
Account access and provisioning	Unit data steward	USAREUR-AF MSS admin team
Data quality and accuracy	Unit data steward	Functional Data Manager
Data governance and policy exceptions	USAREUR-AF C2DAO office (via chain of command)	Army CIO via C2DAO
System outage or application error	USAREUR-AF MSS Help Desk (via unit S6/G6)	MSS program office
Security incident	Unit security officer	Chain of command IAW unit SOP
Application bug or feature request	USAREUR-AF MSS Help Desk (provide application name and error details)	MSS development team via Help Desk

NOTE

Current phone numbers and email addresses for the USAREUR-AF MSS Help Desk and the C2DAO office are maintained by your unit S6/G6 and in your unit SOP. This manual does not list them because they change. Obtain current contact information before you need it.

NOTE

The escalation path for MSS issues follows TM capability levels: (1) SL 1 (Operator) — self-diagnose using Chapter 7 of this manual; use the self-help checklist before escalating. (2) Data Steward — first point of escalation; the steward triages and routes. (3) SL 2 Builder — Workshop application issues, basic pipeline failures, Ontology configuration errors. (4) SL 3 Advanced Builder — complex pipeline design, Ontology architecture, AIP Logic configuration, multi-page application design. (5) SL 4 Developer (code required) — Python/PySpark transforms, TypeScript functions, OSDK development, Agent Studio. Refer to TM-20, Chapter 1 and TM-30, Chapter 1 for role descriptions at each level.

APPENDIX A — QUICK REFERENCE CARD

Print this page. Keep it at your workstation for the first 30 days on MSS.

```
╔══════════════════════════════════════════════════════════════╗
║        MAVEN SMART SYSTEM (MSS) — OPERATOR QUICK REFERENCE   ║
║                    SL 1 / USAREUR-AF                         ║
╚══════════════════════════════════════════════════════════════╝

─── 1. LOG IN ──────────────────────────────────────────────────
Insert CAC → open Chrome or Firefox → navigate to MSS portal URL
Select AUTHENTICATION certificate (not email) → enter PIN
Home screen loads = successful login

If no certificate prompt: remove/reinsert CAC, restart browser, call S6
If PIN rejected 3x: CAC is locked — call S6 immediately

─── 2. FIND YOUR DATA ──────────────────────────────────────────
Search bar (top center) → type name → click result
OR: Compass (left sidebar) → navigate folder tree to unit project

─── 3. READ A DASHBOARD ────────────────────────────────────────
Read metric tiles first → check chart title and legend → read tables
Apply filters to narrow to your unit/date range
CHECK TIMESTAMP — confirm data is current before briefing

─── 4. SUBMIT A FORM ───────────────────────────────────────────
Complete ALL required fields (*) → verify accuracy → click Submit
Wait for green confirmation → screenshot it
Error? Read the message, fix the field, resubmit

─── 5. EXECUTE AN ACTION BUTTON ────────────────────────────────
Select record first (if required) → click button → READ confirmation
dialog carefully → Confirm or Cancel
If unsure what the action does — CANCEL and ask your supervisor

─── 6. AI TOOLS (AIP AGENT) ────────────────────────────────────
Ask specific questions → verify answers against source data
NEVER use AI output in official products without human verification
Report incorrect AI outputs to data steward with screenshot

─── 7. EXPORT DATA ─────────────────────────────────────────────
Export button only → verify authorization first
Handle file IAW classification marking — it does not lose classification
outside MSS. If in doubt: DO NOT EXPORT, contact data steward.

─── 8. SECURITY — ALWAYS ───────────────────────────────────────
Use ONLY your own CAC and PIN
Access ONLY data you are authorized for
LOG OUT before leaving your workstation — every time
See data above your clearance? STOP → close tab → report within 1 hour
```

```
Incorrect data? Report to data steward — do NOT correct it yourself

── 9. WHO TO CALL ──────────────────────────────────────
Login / system problems → Unit S6/G6
Missing access / data issues → Unit Data Steward
Security incident → Supervisor + Security Officer — IMMEDIATELY
App error (with error code) → USAREUR-AF MSS Help Desk via S6/G6
Policy questions → USAREUR-AF C2DAO (via chain of command)
```

APPENDIX B — PROFESSIONAL READING LIST

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

Source	Title	Date	Relevance
Military Review	"Data-Centric at the Division: 3ID's One-Year Journey"	Jan 2025	Unit-level data transformation case study
NCO Journal	"From Data to Wisdom"	Feb 2025	Data literacy fundamentals for leaders
Modern War Institute	"Leadership, Lethality, and Data Literacy"	2024	Strategic case for data literacy
Small Wars Journal	"Data as Firepower"	Aug 2025	Data superiority as warfighting concept
CALL	FY24 MCTP Key Observations	Feb 2025	CTC lessons on data-centric operations

GLOSSARY

20 core terms every MSS operator should know.

Term	Definition
Action	A button or form in a Workshop application that writes data back to MSS when executed. Examples: submitting a SITREP, marking a vehicle as mission capable, approving a request. Actions change live operational records — verify before executing.
AIP (AI Platform)	The AI layer of MSS. Connects large language models to MSS data, enabling natural language queries and automated Logic workflows. AI output must be verified by a human before operational use.
AOR	Area of Responsibility. In MSS, an AOR marking restricts data visibility to users assigned to that geographic or functional area. A user without the AOR marking cannot see that data.
C2DAO	Command Chief Data and Analytics Officer. The USAREUR-AF officer responsible for implementing Army data policy within the command. The C2DAO office is the escalation point for data governance questions and policy exceptions above the unit level.
CAC	Common Access Card. Your personal login credential for MSS. Never share your CAC or PIN with anyone for any reason.
Compass	MSS's file browser. Displays all resources (datasets, applications, projects) organized by folder and project. Used to navigate the platform when you know what folder your data is in.
Contour	MSS's no-code data analysis tool. Allows you to aggregate, filter, sort, and chart data from a dataset without writing any code. Consumer users can perform basic analysis in Contour without builder access.
CUI	Controlled Unclassified Information. Data that requires protection but is not classified. CUI cannot be placed on public-facing systems or transmitted unencrypted. Formerly included FOUO (For Official Use Only), now consolidated under CUI.
Dashboard	A visual display of data in a Workshop application. Includes charts (bar, line, pie), tables (rows and columns), metric tiles (single key numbers), and status indicators.
Data Steward	The person responsible for a specific dataset or application. Your first point of contact for data quality issues, missing access, incorrect records, and questions about data currency. If you do not know who your data steward is, ask your S6.
Dataset	A structured table of data in MSS — rows and columns, like a spreadsheet. Each column has a name and a data type. Each row is one record (one Soldier, one vehicle, one event).
Filter	A control in a dashboard or analysis tool that narrows displayed data to a specific subset — by unit, date range, status, or other field value. Filters affect only your view; they do not change the

Term	Definition
	underlying data.
Foundry	The Palantir software platform on which MSS is built. When you log into MSS, you are logging into Foundry with Army data and Army access controls.
Lineage	The record of where a dataset came from and what processing steps it went through. Use lineage to trace data back to its source system and verify authenticity.
Marking	A label applied to data in MSS that restricts who can see it. Based on classification level (UNCLASSIFIED, CUI, SECRET) and role or AOR restrictions. If you can see marked data in MSS, your assigned markings authorize you to see it.
MSS	Maven Smart System. USAREUR-AF's operational data and AI platform, built on Palantir Foundry. The command's single integrated environment for readiness visibility, operational reporting, logistics tracking, and personnel accountability.
Ontology	The semantic layer of MSS. Defines what data represents in terms of real-world things — Soldiers, units, vehicles, reports — and how those things are connected to each other. Viewed through Quiver.
Project	A workspace in MSS containing related datasets, applications, and resources for a specific unit or mission area. Your access is limited to the projects your account has been granted.
Quiver	MSS's ontology exploration tool. Allows you to browse objects (units, Soldiers, vehicles) and their relationships without writing queries. Consumer users can view and filter objects in Quiver.
Workshop	MSS's application layer — the interface most users see. Dashboards, forms, maps, and reports built by developers and published for unit use. Workshop is where most day-to-day MSS activity happens for consumer users.

SL 1 — Maven Smart System (MSS) Operator Technical Manual HEADQUARTERS, UNITED STATES ARMY EUROPE AND AFRICA, Wiesbaden, Germany 2026 For corrections or updates, contact the USAREUR-AF Operational Data Team through your unit data steward or the C2DAO office.