TECHNICAL MANUAL

SL 4E

USAREUR-AF

TM-40E — MAVEN SMART SYSTEM (MSS)

Specialist Course Manual

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

26 MARCH 2026

DRAFT — UNOFFICIAL — NOT FOR OPERATIONAL USE

TM-40E — MAVEN SMART SYSTEM (MSS)

Forward: SL 4E teaches Protection WFF practitioners — CBRN officers, AT officers, Military Police, ADA officers, and support engineers — how to use MSS in daily protection work. The focus is operational use of MSS to accomplish protection tasks aligned to ADP 3-37 and subordinate doctrine. No coding, no pipeline development, no transform experience required. **Prereqs:** SL 1, Maven User; SL 2, Builder; SL 3, Advanced Builder; CONCEPTS_GUIDE_TM40E_PROTECTION (required before beginning this manual).
HQ USAREUR-AF · v1.0 · 2026 · DISTRIB: USG only · AUTH: C2DAO/UDRA v1.1

WARNING: Presenting CBRN hazard data without verifying currency and source validation can direct Soldiers into contaminated areas. Always confirm CBRN overlay data-as-of timestamp and originating sensor or report before disseminating. A contamination overlay that is hours old may no longer reflect actual hazard boundaries. WARNING: Do NOT use MSS engagement data to make C-UAS engagement decisions without confirmation through the established engagement authority chain. MSS data is a tracking tool — it does not replace engagement authority procedures under ATP 3-01.81 and theater ROE. CAUTION: MSS FPCON alert notifications are threshold-based and depend on AT officer data entry. An automated FPCON alert is a prompt to verify the current command-directed FPCON — not a substitute for the commander's authority to establish and communicate FPCON levels. NOTE: MSS does not replace physical protection measures. No data platform can substitute for guard posts, physical barriers, patrols, CBRN detection equipment, or the judgment of experienced protection professionals. MSS integrates and displays information about those measures. The measures themselves must exist in the physical domain.

CHAPTER 1 — OVERVIEW AND THE PROTECTION WARFIGHTING FUNCTION IN MSS

BLUF: SL 4E teaches Protection WFF practitioners — CBRN officers, AT officers, Military Police, ADA officers, and support engineers — how to use MSS in daily protection work. The focus is operational use of MSS to accomplish protection tasks aligned to ADP 3-37 and subordinate doctrine. No coding, no pipeline development, no transform experience required.

1-1. Protection Specialist Manual

The protection WFF preserves the force and its freedom of action (ADP 3-37, para 1-1). Protection encompasses all tasks that protect friendly forces, civilian partners, and critical infrastructure from all threats and hazards — kinetic, CBRN, electronic, physical, and psychological. Commanders and staffs integrate, synchronize, and direct protection activities as part of the operations process to preserve combat power across all phases of the operation.

MSS does not change the purpose or doctrinal tasks of the protection WFF. It changes how rapidly protection data is aggregated, correlated, and disseminated across the formation. A protection cell that formerly tracked CBRN events on paper overlays, AT vulnerability data in disconnected spreadsheets, and FPCON changes through voice reporting can use MSS to integrate those data streams in near real time — and push current protection pictures to subordinate commanders without delay.

The USAREUR-AF C2DAO built MSS on Palantir Foundry to integrate operational data streams, including protection data, into a single enterprise platform. Protection data on MSS includes threat feeds relevant to force protection, CBRN event and hazard data, physical security data, AT assessment data, AMD warning data, and survivability tracking. These data streams, previously managed in separate systems or not digitally managed at all, converge in MSS into an integrated protection operating picture.

NOTE: MSS is a protection data integration enabler. It does not replace protection doctrine, the Protection Working Group, or the authority and judgment of the AT officer, CBRN officer, PMO, or protection officer. Those positions own their protection tasks. MSS provides the data layer that supports those tasks.

1-2. The ADP 3-37 Protection Tasks and MSS Data

ADP 3-37 organizes protection into tasks conducted by the force as a whole. Table 1-1 maps those tasks to MSS data domains.

Table 1-1. Protection Tasks and MSS Data Domains (IAW ADP 3-37)

Protection Task	Doctrinal Reference	Primary MSS Data Domain	Primary User
Conduct Composite Risk Management	FM 5-19	Risk assessment tracking workspace	All leaders
Conduct CBRN Defense	FM 3-11 series	CBRN event/hazard layer	74A/74D
Conduct Antiterrorism	ATP 3-37.2	AT assessment, FPCON, RAM workspace	AT Officer
Conduct Physical Security Operations	AR 190-13	ECP, access control, perimeter layer	31A/31B

Protection Task	Doctrinal Reference	Primary MSS Data Domain	Primary User
Conduct Air and Missile Defense	FM 3-01 series	AMD air picture, CAL/DAL workspace	14A/14P/14S
Conduct Internment/Resettlement	FM 3-39 series	Detainee tracking (coord with PMO)	31A/31D
Conduct Chemical, Biological, Radiological, and Nuclear Operations	FM 3-11	CBRN planning data	74A/74D
Employ Safety Techniques	DA Pam 385-10	CRM data, accident prevention tracking	Safety officer
Implement Operational Security	FM 3-13.3	OPSEC risk data, MISO coordination	S3, IO, 37F
Conduct Personnel Recovery	JP 3-50	Personnel recovery tracking	G1/S1 coordination
Provide Survivability Operations	ATP 3-37.34	Fighting position, hardening status layer	12B/12R
Conduct Base Camp Planning and Design	ATP 3-37.10	Base camp design data layer	12B/12R/PM

1-2a. Protection Data Flow in MSS — How Information Moves

Understanding how protection data flows in MSS helps practitioners identify where data integration breaks down. Figure 1-1 describes the data flow in text form.

Protection Data Flow (Text Description):

1. **Data entry at the source.** CBRN events are entered by the CBRN NCO at the point of detection. MP incidents are entered by the desk officer at the ECP or PMO office. AT incidents are entered by the AT officer. Each practitioner enters data in their functional zone.
2. **Integration into the shared protection workspace.** Each functional zone contributes its data to the shared protection workspace. The contamination overlay from the CBRN zone becomes visible to the S2, S3, and subordinate units. The FPCON level from the AT zone is visible to all units in the workspace. The ECP status from the PMO zone informs the base defense picture.
3. **Consumption by adjacent WFF practitioners.** The S3 (Mission Command WFF) consumes the protection picture as part of the COP. The S2 contributes threat data to the AT assessment and receives protection data for intelligence integration. The S4 coordinates with the CBRN zone for decontamination resupply requirements. The engineer section coordinates with the survivability zone.

4. **Reporting up the chain.** Protection data that meets reporting thresholds (SIRs, NBC reports, AT incidents) feeds into the formation's reporting products. MSS provides the data record that supports upward reporting — but the AT officer or PMO must still generate the formal report through the appropriate channel.
5. **Feedback from higher.** FPCON changes, ADW changes, and theater AT assessments flow down from higher formations into the unit protection workspace. The AT officer verifies receipt and updates the unit's workspace.

Data quality failures most commonly occur at Steps 1 and 2 — data is not entered at the source, or it is entered but not shared with the broader workspace. The protection officer's data quality role focuses on these two steps.

1-3. MSS vs. Legacy Protection Tools

Before MSS, protection practitioners managed data across fragmented systems: CBRN tracking in JCAD logs and paper overlays, AT data in unit-level spreadsheets, MP incident data in paper blotters, and AMD warning data in voice-only reporting chains. Table 1-2 shows the MSS equivalents.

Table 1-2. Legacy Protection Tools vs. MSS

Legacy Tool / Method	MSS Equivalent	Improvement
Paper CBRN contamination overlays	CBRN hazard overlay layer in MSS	Shareable across echelons in near real time
AT vulnerability assessment spreadsheets	AT assessment workspace in MSS	Version-controlled, linked to FPCON data
MP blotter (paper/local spreadsheet)	Incident and SIR tracking dashboard	Integrated with force protection picture
Voice-only FPCON reporting chain	FPCON status layer, alert notification	Documented change log, automated notification
AMD voice reporting net (SHORAD warning)	AMD air picture and ADW tracking layer	Integrated with threat correlation data
Manual RAM tracking on whiteboard	RAM management workspace	Searchable, scheduled, execution-traceable
Paper CRM worksheets	CRM risk assessment workspace	Linked to unit tasks, archived for trend analysis
Disconnected survivability position sketches	Survivability position data layer	Geospatially integrated with base camp design data

1-4. Protection Workspace Organization

The MSS protection workspace is organized around the Protection Working Group (PWG) data structure. The PWG, chaired by the protection officer (or G3/S3 at echelons without a designated protection officer), synchronizes all protection-related data contributions from CBRN, PMO, AT, AMD, legal, and engineer cells.

Protection Workspace Zones: - **CBRN Cell Zone** — CBRN threat data, contamination overlays, detection equipment status, decontamination site tracking - **PMO Zone** — MP incident data, ECP status, access control records, SIR tracking - **AT Officer Zone** — Threat vulnerability assessments, FPCON levels, RAM schedule and execution data, AT lessons learned - **AMD Cell Zone** — Air picture, CAL/DAL management, ADW status, SHORAD sector data - **Survivability Zone** — Fighting position status, facility hardening data, CCD planning data

NOTE: Not all units will have designated personnel for every workspace zone. Smaller units should consolidate protection workspace management under the highest-ranking available protection-qualified officer or NCO. Coordinate with the parent formation's protection cell for workspace templates and data standards.

1-4a. Doctrinal References Summary

SL 4E aligns to multiple doctrinal publications. Table 1-4 provides a quick reference to the primary doctrinal sources for each protection domain covered in this manual.

Table 1-4. Doctrinal References by Protection Domain

Domain	Primary Reference	Key Paragraphs/Sections	MSS Chapter
Protection WFF Overview	ADP 3-37, FM 3-37	ADP 3-37 Ch.1–2; FM 3-37 Ch.1–3 (protection tasks, integration, assessment)	1
Composite Risk Management	FM 5-19	Para 1-2 (5-step process), Ch.2 (hazard assessment), Ch.4 (risk acceptance authority)	2
CBRN Defense	FM 3-11, FM 3-11.9, ATP 3-11.32	FM 3-11 Ch.3 (CBRN tasks); FM 3-11.9 (hazard prediction); ATP 3-11.32 (CBRN OPDS)	3
NBC Reporting	FM 3-11, ATP 3-11.37	FM 3-11 Ch.4 (CBRN reporting); NBC 1–6 formats	3, Appendix B
Antiterrorism	ATP 3-37.2, DOD O-2000.12-H	ATP 3-37.2 Ch.2 (AT methodology), Ch.3 (vulnerability assessment)	4
FPCON	DOD O-2000.12-H, ATP 3-37.2	DOD O-2000.12-H Encl.4 (FPCON measures)	4, Appendix

Domain	Primary Reference	Key Paragraphs/Sections	MSS Chapter
			C
Physical Security	AR 190-13, AR 190-51	AR 190-13 Ch.2 (physical security program)	5
Serious Incident Reporting	AR 190-40	AR 190-40 Ch.3 (SIR categories and timelines)	5
Air and Missile Defense	ADP 3-01, FM 3-01	ADP 3-01 para 1-1 (AMD purpose); FM 3-01 Ch.2 (AMD tasks)	6
CAL/DAL	FM 3-01, ADP 3-37	FM 3-01 para 2-3 (CAL/DAL process)	6
Electronic Warfare	FM 3-36	FM 3-36 Ch.2 (EW tasks), Ch.4 (EW in protection)	7
Counter-UAS	ATP 3-01.81	ATP 3-01.81 (C-UAS operations)	7
Survivability Operations	ATP 3-37.34	ATP 3-37.34 Ch.2 (survivability planning), Ch.3 (construction standards)	8
Base Camp Design	ATP 3-37.10	ATP 3-37.10 Ch.3 (force protection in base camp design)	8
Echelon Operations	ADP 3-37, ADP 3-90	ADP 3-37 Ch.4 (echelon protection tasks)	9
OPSEC	FM 3-13.3	FM 3-13.3 Ch.2 (OPSEC process)	All
Protection Program	AR 525-2 (Jun 2023)	Overarching protection regulation	All
OPSEC Regulation	AR 530-1 (Sep 2014)	Primary OPSEC regulation	All
OPSEC TTP	ATP 3-13.3	OPSEC tactics, techniques, and procedures	All
Geospatial Engineering	FM 3-34	GMAD framework (Generate-Manage-Analyze-Disseminate)	8
Cyberspace/EW	FM 3-12	Cyber component of protection WFF	7

Strategic Guidance:

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

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

1-5. Scope: What SL 4E Covers and Does Not Cover

SL 4E covers operational use of MSS for CBRN defense, AT, physical security, AMD coordination, EW awareness, survivability tracking, and CRM; Protection Working Group data management on MSS; FPCON management, RAM tracking, AT assessment data management; CBRN event reporting, contamination overlay management, detection equipment status tracking; echelon-specific guidance for company through division/corps protection cells; and degraded operations procedures and fallback products.

SL 4E does NOT cover pipeline construction, data transforms, or code development — see SL 3 and SL 4L; building Workshop dashboards — see SL 2; intelligence analysis methods — see SL 4A; kinetic fires coordination — see SL 4B; information operations development — see IO officer / G7 coordination; or medical/CASEVAC tracking — see SL 4D (Sustainment).

1-6. MOS Coverage and Audience

Table 1-3. Primary Audience by MOS and Position

MOS	Title	Position	Primary Chapters
74A	CBRN Officer	CBRN Officer, Chemical Officer	1, 2, 3, 8, 9, 10
74D	CBRN Specialist	CBRN NCO, CBRN Recon Specialist	3, 8, 9
31A	Military Police Officer	PMO, Provost Marshal, Desk Officer	1, 4, 5, 9, 10
31B	Military Police	MP, Gate Guard, Patrol	5, 9
31D	Criminal Investigate Agent	CID Special Agent	4, 5
14A	ADA Officer	ADA Battery Commander, AMD Officer	6, 9
14E	Patriot Fire Control Operator	Patriot FCS Operator/Maintainer	6
14P	Air Defense EWS Operator	AEWS Operator	6
14S	AMD Crewmember	AMD Crew, Avenger/Shorad	6, 9

MOS	Title	Position	Primary Chapters
12B	Combat Engineer	Combat Engineer, Sapper	8, 9
12R	Interior Electrician	Base Camp Electrician	8
27A	Judge Advocate	SJA, Legal Advisor	4, 5
37F	PSYOP Specialist	MISO Team, PSYOP NCO	4
180A	SF Warrant Officer	18-Series (base defense focus)	4, 5, 8
311A/311B	CI Warrant/Agent	COUNTERINT, CI Special Agent	4

1-7. Relationship to Other TMs in the MSS Curriculum

Table 1-5. TM Curriculum Relationships

TM	Title	Relationship to SL 4E
SL 1	Maven User	Foundation prerequisite. Platform navigation, basic data access. Required before this manual.
SL 2	Builder	Required as prerequisite (Go evaluation on file). Builder skills are not exercised in this track — SL 4E practitioners consume pre-built products. The SL 2 cert is part of the progression chain to SL 3.
SL 3	Advanced Builder	Required prerequisite (Go evaluation on file). Advanced builder skills are not exercised in this track — SL 4E practitioners consume pre-built products. SL 3 completion certifies platform literacy at the level required before WFF track enrollment.
SL 4A	Intelligence	Companion. Threat data from Intel feeds AT risk assessments; protection posture feeds intelligence picture.
SL 4B	Fires	Companion. AMD coordination (Ch. 6) requires fires WFF integration; C-UAS engagement data crosses both domains.
SL 4C	Movement and Maneuver	Companion. Route security and convoy protection integrate protection and maneuver data; survivability positions support maneuver units.
SL 4D	Sustainment	Complementary. CBRN decontamination requires sustainment coordination; force protection affects supply route security.
SL 4E	Protection	This manual.
SL 4F	Mission Command	Complementary. Protection picture feeds the COP (S3 product); FPCON and SIR data feeds commander CCIR monitoring.

TM	Title	Relationship to SL 4E
SL 5G–O	Advanced Specialist Tracks	Post-graduate level for technical specialists (prereq SL 4G–O). Not applicable to operational protection practitioners.

NOTE: SL 2 and SL 3 are required as prerequisites (Go evaluations on file) but builder skills are not exercised in this manual. SL 4E assumes no ability to build pipelines or transforms. If you encounter a protection data product that does not exist and needs to be built, coordinate with your unit's designated MSS Builder (SL 3 qualified) or the C2DAO.

CHAPTER 2 — COMPOSITE RISK MANAGEMENT IN MSS

BLUF: FM 5-19 Composite Risk Management (CRM) is a five-step process all leaders execute. MSS provides a structured workspace to document, track, and archive CRM data — converting what was formerly a paper-based process into a searchable, shareable record that supports trend analysis and accident prevention.

2-1. CRM Overview and MSS Integration

CRM is the Army's primary process for managing risk. The five steps are: identify hazards; assess hazards; develop controls; implement controls; and supervise and evaluate (FM 5-19, para 1-2). All leaders conduct CRM for training, operations, and maintenance tasks. MSS does not change the process — it provides the data infrastructure to execute and track CRM at unit level.

Before MSS, CRM worksheets existed as paper products, local files, or disconnected forms. Unit safety officers had no mechanism to aggregate CRM data across subordinate formations or identify recurring hazard trends. MSS addresses this by providing a centralized CRM workspace where risk assessment data is entered, reviewed by approving authority, archived, and available for trend analysis.

NOTE: MSS CRM data entry does not satisfy the requirement to brief leaders and Soldiers on identified hazards and controls. CRM in MSS supports documentation and tracking. The actual risk communication — briefings, rehearsals, pre-execution checks — remains a leader responsibility in the physical domain.

2-2. Hazard Identification in MSS

TASK: Conduct Hazard Identification and Enter Data in MSS

CONDITIONS: Unit has a planned training or operational task. Safety officer or NCO has CRM workspace access in MSS. Relevant mission parameters (terrain, weather, task description, equipment, personnel experience level) are known.

STANDARDS: All mission and environmental hazards for the planned task are entered in the MSS CRM workspace. Each hazard record includes: hazard description, hazard category (mission or environmental), task phase when hazard is present, and potential consequences. Hazard identification is complete NLT 24 hours before task execution for routine training; NLT 4 hours for time-constrained operations.

PROCEDURE: 1. Navigate to the unit CRM workspace in MSS. Verify workspace is the correct echelon (company, battalion, brigade) before entering data. 2. Select "New Risk Assessment" and enter the task name, date, and approving authority. 3. For each identified hazard, select "Add Hazard" and enter: a. Hazard description (specific, not generic — "black ice on MSR PHOENIX at Grid XX" not "weather") b. Hazard category: Mission (task-related), Environmental (terrain, weather, infrastructure), or Personnel (experience, training level, fatigue) c. Phase of the task when the hazard is present d. Potential consequence if the hazard results in an incident (injury type/severity, equipment damage, mission failure) 4. Save each hazard entry. The system timestamps and attributes the entry to the entering user. 5. Coordinate with the approving authority to review the hazard list before proceeding to assessment.

2-2a. Hazard Categories in MSS — Common Errors and Corrections

Protection practitioners frequently make two errors in hazard identification data that degrade the value of the CRM record. The first is using generic hazard descriptions. The second is using the wrong hazard category.

Table 2-3. Hazard Description Quality Examples

Category	Poor Entry (Generic)	Correct Entry (Specific)
Environmental	"Bad weather"	"Freezing rain forecast 0200–0600; road surface on MSR VIKING will be ice-covered; road grade >8% at grid XY123456"
Mission	"Equipment hazard"	"M1089 recovery vehicle boom may contact overhead power lines during vehicle recovery operations at grid YZ789012 — power lines at 18 feet"
Personnel	"Inexperienced Soldiers"	"12 of 23 Soldiers in the platoon have not completed NVG qualification; night driving on this route is required for this mission"
Environmental	"Hot weather"	"WBGT index forecast 95°F+ during afternoon portion of task (1300–1700); task requires sustained moderate-to-heavy physical exertion without shade"
Mission	"Dangerous operation"	"MOUT training facility has live fire range 400m from assault course; potential for ricochet to reach training assembly area if range fails to provide warning

Category	Poor Entry (Generic)	Correct Entry (Specific)
		of live fire activity"

Common Hazard Category Errors: - Categorizing personnel factors as mission factors. The difference: a mission factor relates to the task itself; a personnel factor relates to the people executing it. An inexperienced Soldier is a personnel hazard. The task requiring night operations is a mission hazard. - Failing to enter environmental hazards for weather-dependent tasks. Every task with a weather envelope (helicopter operations, vehicle movement in snow, decontamination in extreme cold) requires a weather/environmental hazard entry. - Listing "enemy action" as a hazard without specificity. In an operational environment, threat contact is a hazard. The specific threat form (IED on the route, threat drone activity, direct fire from a specific direction) is the hazard — not the generic category.

2-3. Hazard Assessment and Risk Scoring

Hazard assessment in MSS uses the Army's standard risk matrix: Probability (Frequent, Likely, Occasional, Seldom, Unlikely) × Severity (Catastrophic, Critical, Marginal, Negligible) = Risk Level (High, Significant, Moderate, Low) (FM 5-19, Table 2-2).

Table 2-1. Army Risk Assessment Matrix (FM 5-19)

Probability \ Severity	Catastrophic	Critical	Marginal	Negligible
Frequent	High	High	Significant	Moderate
Likely	High	High	Significant	Moderate
Occasional	High	Significant	Moderate	Low
Seldom	Significant	Moderate	Moderate	Low
Unlikely	Moderate	Moderate	Low	Low

In the MSS CRM workspace, the risk matrix is embedded as a selector tool. After entering the probability and severity for each hazard, MSS automatically calculates and displays the risk level. This eliminates manual matrix lookup errors and ensures consistent scoring across the formation.

CAUTION: MSS risk scoring is only as accurate as the probability and severity entries. Leaders must apply professional judgment — not just select the lowest risk category to expedite approval. A consistent pattern of underscored risk assessments will be visible in trend analysis and reflects poorly on unit safety culture.

2-4. Risk Control Measures — Entry, Tracking, and Verification

TASK: Enter and Track Risk Control Measures in MSS

CONDITIONS: Hazard identification and assessment are complete in the MSS CRM workspace. Approving authority has reviewed the hazard list. Control measures have been determined through leader analysis.

STANDARDS: Each identified hazard has at least one control measure entered in MSS. Each control record includes: control measure description, control type (Eliminate, Avoid, Control, Accept), responsible person (name or position), implementation deadline, and verification method. No hazard with a residual risk rating of High proceeds without approving authority notation in MSS.

PROCEDURE: 1. For each hazard in the risk assessment, select "Add Control Measure." 2. Enter the control measure description. Controls must be specific and actionable ("reduce convoy speed to 25 MPH on ice-affected segments of MSR PHOENIX" — not "drive carefully"). 3. Select control type: - Eliminate: Remove the hazard entirely (change route, cancel task phase) - Avoid: Schedule task to avoid hazard (daylight only, non-icy conditions) - Control: Implement measure to reduce probability or severity - Accept: Acknowledge hazard with no additional control (requires approving authority sign-off in MSS) 4. Assign responsible position and implementation deadline. 5. Enter verification method — how the leader will confirm the control was implemented (PCCs/PCIs, inspection, brief-back). 6. After all controls are entered, MSS calculates residual risk for each hazard. Review residual risk with approving authority. 7. Approving authority signs the assessment in MSS. For High residual risk assessments, the system requires annotated acceptance with reason. 8. After task execution, return to the risk assessment and mark each control "Verified" or "Not Verified" with a brief note. This data feeds unit trend analysis.

2-5. Residual Risk Acceptance and Approving Authority Documentation

MSS captures the residual risk acceptance chain. The approving authority for risk acceptance is determined by the residual risk level (FM 5-19, para 4-3):

Table 2-2. Risk Acceptance Authority (FM 5-19)

Residual Risk Level	Approving Authority
Low	Squad/Section leader (SSG and above)
Moderate	Company/Battery Commander
Significant	Battalion Commander
High	Brigade Commander or higher

MSS enforces this chain by requiring electronic signature from the appropriate authority level before the assessment is finalized. If the authority has not signed and the task is imminent, the unit must escalate through command channels — not proceed with an unsigned High-risk assessment.

NOTE: MSS does not prevent a unit from executing a task with unsigned risk documentation — it records the state of the approval chain. Leaders and commanders remain responsible for ensuring proper risk acceptance before execution. MSS provides the audit trail.

2-5a. Residual Risk Acceptance — Annotated Example

The following example shows a correctly completed residual risk acceptance entry in MSS for a High-residual-risk assessment.

Scenario: 2-12 CAV Squadron is conducting a night convoy on a mountain route in freezing conditions to resupply COP BRAVO. The risk assessment produces a High residual risk based on ice, reduced visibility, and distance from Role 2 medical support.

MSS Entry Fields (example):

Field	Entry
Task	Night convoy MSR PHOENIX to COP BRAVO
Date	14 MAR 26
Risk assessment author	SSG MORGAN, Safety NCO
Initial risk level	High
Hazards identified	Black ice on descending grades, night driving in reduced visibility, 90-minute medevac range
Controls	Reduce speed to 20 MPH on descent grades; NODS mandatory for all vehicle commanders; Medical track as chalk 3; GO/NO-GO criteria: visibility below 400m = mission abort; SFC PRICE designated ground guide for switchback turns
Residual risk level	High (unavoidable given terrain and mission requirement)
Accepted risk rationale	COP BRAVO resupply is a mission requirement — no alternate route or timing window reduces terrain risk below High. Medical track inclusion and abort criteria reduce likelihood of catastrophic outcome. Commander accepts residual risk IAW FM 5-19, para 4-3.
Approving authority	LTC BARKER, 2-12 CAV, 131200Z MAR 26
Electronic signature	LTC BARKER (confirmed in MSS)

NOTE: The approving authority's acceptance entry must include the rationale — not just a signature. A High-risk assessment signed without rationale does not provide the data record that demonstrates command engagement with the risk. When reviewing subordinate CRM data, protection officers and safety officers should flag signed-but-unexplained High-risk acceptances as data quality issues.

2-6. Training Accident Prevention — Trend Data Use

One of the greatest value-adds MSS provides over legacy CRM processes is trend analysis. When risk assessment data from multiple units and multiple cycles exists in the same workspace, the safety officer can identify recurring hazards, control measures that consistently fail verification, and task categories that generate disproportionate risk.

Using CRM Trend Data in MSS: - Navigate to the Safety Officer trend view in the CRM workspace. - Filter by task type, date range, or unit to identify recurring hazards. - Review control verification data to identify controls that are routinely entered but rarely verified — these represent CRM compliance gaps. - Use trend data to inform quarterly safety briefings, unit safety stand-downs, and command safety reports. - Export trend summaries for submission to the brigade or division safety officer for formation-wide analysis.

CHAPTER 3 — CBRN DEFENSE OPERATIONS

BLUF: 74A CBRN officers and 74D CBRN specialists use MSS to manage CBRN threat data, maintain contamination overlays, track detection equipment status, manage decontamination sites, and report CBRN events using NBC 1–6 report formats. MSS is the primary data integration platform for CBRN defense within the USAREUR-AF formation.

WARNING: CBRN data errors can result in Soldiers entering contaminated areas without personal protective equipment. All CBRN data entered in MSS must be sourced from confirmed sensor readings, laboratory results, or validated reports — not assumed or estimated. Label all CBRN data with source, confidence level, and data-as-of timestamp.

3-1. CBRN Officer/Specialist Workflow in MSS

The CBRN cell's primary data responsibilities in MSS are: 1. Maintain the current CBRN threat data layer (contamination overlays, hazard predictions) 2. Track CBRN reports (NBC 1–6) as structured data entries 3. Monitor detection equipment status 4. Track decontamination site readiness 5. Track CBRN casualties and patient movement coordination with medical

The CBRN workspace in MSS is organized around these five functional areas. Navigate to the CBRN cell zone within the unit protection workspace to access each area.

3-2. CBRN Threat Data Management

CBRN threat data in MSS encompasses two categories: confirmed event data (actual detonations, releases, or sensor detections) and predictive/templated data (hazard prediction model outputs, threat capability assessments).

Confirmed CBRN event data fields in MSS: - Event type: Chemical, Biological, Radiological, Nuclear - Agent (if identified): specific agent or "unknown agent" — do not guess - Detection method: M8A1 automatic alarm, M256A2 detection kit, biological detection, radiation dosimeter, laboratory analysis - Location: grid coordinate (8-digit minimum), accuracy estimate - Time of detection (DTG, Zulu) - Wind direction and speed at time of detection (from met data or field observation) - Reported by (unit, position, callsign) - Confidence level: Confirmed, Probable, Suspected

Hazard prediction data fields in MSS: - Prediction model used (HPAC, D2Puff, manual calculations IAW FM 3-11.9) - Input parameters: agent type, release quantity (if known), meteorological data - Hazard area overlay (loaded as a geospatial layer, not free-text) - Prediction validity period (time-based — met data degrades prediction accuracy rapidly) - Model run time (DTG)

CAUTION: Hazard prediction overlays have a limited validity period based on meteorological conditions. When wind direction or speed changes more than 10 degrees or 3 knots, re-run the hazard prediction and update the MSS overlay. A stale hazard prediction is dangerous if used for route planning or personnel movement decisions.

3-3. Contamination Control Point Tracking in MSS

TASK: Establish and Track a Contamination Control Point (CCP) in MSS

CONDITIONS: A CBRN event has occurred or is suspected. The CBRN officer has directed establishment of a CCP. CBRN workspace access is active in MSS.

STANDARDS: The CCP is entered as an active geospatial object in the MSS CBRN layer within 15 minutes of CCP establishment. The entry includes CCP grid, type (hasty or deliberate), decontamination capability (personnel/equipment), capacity (personnel per hour), operational status, and CBRN NCO in charge. CCP status is updated minimum every 4 hours while the CCP remains active.

PROCEDURE: 1. Navigate to the CBRN cell zone in the unit protection workspace. 2. Select "New CCP Entry" from the contamination control layer. 3. Enter CCP location as an 8-digit grid coordinate. Plot on the CBRN geospatial layer. 4. Select CCP type: Hasty (field-expedient, rapidly established) or Deliberate (engineer-improved, sustained capacity). 5. Enter decontamination capability: Personnel Only, Equipment Only, or Personnel and Equipment. 6. Enter estimated capacity (personnel per hour) based on available

assets and decontamination unit capability. 7. Set operational status: Active, Stand-by, or Closed. 8. Enter the responsible CBRN NCO name and callsign. 9. Link the CCP entry to the originating CBRN event report if applicable. 10. Brief the protection officer and S3 on CCP status. Confirm the CCP location is reflected in the CBRN overlay that subordinate units can access.

3-4. CBRN Reporting — NBC 1–6 Reports in MSS

MSS provides structured data entry forms for all six NBC report types. These forms enforce format compliance and push report data into the CBRN data layer for immediate integration with the protection operating picture. Appendix B provides quick reference format cards for each report type.

NBC Report Types and MSS Entry:

Report	Purpose	Triggers MSS Entry	Auto-Populated to CBRN Layer
NBC 1	Initial CBRN event — observer report	On observer report receipt	Yes — event marker
NBC 2	Evaluated data — staff-processed	After S2/CBRN evaluation	Yes — updates event marker
NBC 3	Immediate warning of CBRN attack	Immediately on attack	Yes — alert notification
NBC 4	Reconnaissance and monitoring	After recon/monitoring results	Yes — updates hazard area
NBC 5	CBRN zone summary	After hazard prediction complete	Yes — hazard overlay
NBC 6	Detailed technical data	After laboratory/technical analysis	Yes — agent identification field

NOTE: NBC 3 reports in MSS trigger an automatic alert notification to all units in the shared protection workspace. Verify that the NBC 3 data is accurate and command-directed before entry. A false NBC 3 report will trigger unit protective actions across the formation.

3-4a. Common NBC Report Entry Errors

The following errors are the most commonly observed in NBC report entries in MSS. The CBRN officer should brief these to 74D CBRN specialists before initial MSS use.

Table 3-2. Common NBC Report Data Entry Errors

Error	Description	Correction
DTG is entry time, not event time	Soldier enters current time rather than the time of the actual CBRN detection or event	Always use the actual event DTG. If event time is unknown, enter "UNKOWN" and document the best estimate
Grid is observer location, not event location	Observer enters their own position rather than the location of the CBRN event	NBC 1 Line 3 is the attack/event location, not the observer location
Agent listed as "CBRN" or "unknown chemical"	Placeholder entries that carry no actionable information	Enter the most specific known description: if truly unknown, enter "UNKNOWN AGENT" as a complete phrase, not an abbreviation
Met data missing or undated	Hazard predictions are entered without the meteorological data used, making the prediction unverifiable	Always include met data source (field observation, METOC report, nearest weather station), wind direction and speed, stability class if used
Confidence level defaulted to "Suspected"	All entries are marked "Suspected" regardless of the actual evidentiary basis	Use the correct confidence level: Confirmed = laboratory or definitive technical analysis; Probable = strong sensor indication + symptom correlation; Suspected = single sensor or unconfirmed report

3-5. Detection Equipment Status Tracking

The CBRN officer tracks detection equipment status in MSS to maintain visibility on CBRN detection capability across the formation. This data informs protection planning — gaps in detection coverage must be addressed through repositioning, supplemental detection assets, or adjusted routes.

Detection Equipment Status Fields: - Equipment type (M8A1, JCAD, MINICAD, RAID-M, AN/UDR-13, biological detection system) - Assigned unit and grid location - Operational status: FMC (fully mission capable), PMC (partially mission capable), NMC (non-mission capable) - Battery/power status - Last calibration/service date - Responsible operator (name and position) - Estimated return to FMC for NMC equipment

Maintain a detection equipment dashboard in the CBRN workspace. Brief detection capability gaps at the Protection Working Group.

3-6. Decontamination Site Management

Decontamination site data in MSS mirrors CCP tracking but at a larger scale — typically the decontamination platoon or company's operational sites rather than hasty field CCPs.

Decontamination Site Data Fields: - Site type (thorough decontamination, operational decontamination, MOPP gear exchange) - Location (grid, plus approach and exit route data) - Water source (location, distance from site, quantity available) - Throughput capacity (vehicles per hour, personnel per hour) - Operational status - Parent unit providing decontamination capability - Support request link (if external decontamination unit is supporting)

3-7. Issuing a CBRN Warning to Subordinate Units in MSS

The most time-critical CBRN data action is warning subordinate units of an active CBRN hazard. MSS enables simultaneous warning through the NBC 3 notification function. The procedure must be executed without delay — every minute between event and warning is a minute in which subordinates may be moving through or toward a hazard area.

TASK: Issue a CBRN Warning to Subordinate Units via MSS

CONDITIONS: A CBRN event has been detected or reported. The NBC 1 report has been received and evaluated. The CBRN officer has determined a warning is required (NBC 3). MSS CBRN workspace access is active. Subordinate units are in the shared protection workspace.

STANDARDS: NBC 3 warning data is entered in MSS and notification transmitted within 10 minutes of the decision to warn. The hazard area is plotted as a geospatial overlay, not described in text only. Notification reaches all affected subordinate units in the shared workspace. Parallel voice warning is transmitted on the NBC reporting net simultaneously with MSS entry.

PROCEDURE: 1. Navigate to the CBRN zone. Select "Issue NBC 3 Warning." 2. Enter hazard type: Nuclear, Biological, Chemical, Radiological. 3. Enter agent (if identified) or "UNKNOWN AGENT." Do not leave blank — use "UNKNOWN" rather than guess. 4. Enter hazard center point grid (location of event, not assumed drift point). 5. Plot the predicted hazard boundary using the hazard prediction tool (Chapter 3, para 3-2) or manually from FM 3-11.9 calculations. The hazard boundary must be a geospatial shape, not a radial distance description. 6. Enter recommended protective actions for personnel in the hazard area and adjacent areas: - MOPP level (MOPP READY, MOPP 1, 2, 3, or 4 as appropriate) - Avoid, shelter, evacuate, or continue mission as applicable - Route guidance if applicable 7. Enter hazard validity: current met data validity (typically 1–3 hours; re-run prediction when met data updates). 8. Set notification recipients: all subordinate units, adjacent units, parent formation as applicable. 9. Issue MSS notification. Simultaneously transmit voice warning on NBC reporting net — do not wait for MSS confirmation before going to voice. 10. Monitor NBC reporting net for acknowledgement from subordinate units. If any unit fails to acknowledge within 10 minutes, notify their higher by voice.

WARNING: Transmitting a false NBC 3 warning in MSS will trigger immediate MOPP transitions across the formation. The disruption to operations and the risk of heat casualties from unnecessary MOPP transitions make false NBC 3 reports operationally dangerous. Verify the

event before issuing NBC 3 — but do not delay an accurate NBC 3 for confirmation processes that take longer than the urgency of the warning allows.

3-8. CBRN Casualty Tracking

CBRN casualties require coordination between the CBRN cell, medical, and the S1. MSS tracks CBRN casualties as a distinct casualty category within the CBRN workspace, linked to the broader personnel tracking system.

CBRN Casualty Data Fields: - Casualty name, rank, unit - CBRN casualty category: contaminated (no symptoms), CBRN symptomatic, CBRN confirmed - Agent exposure (if known) - Time of exposure (DTG) - Treatment received (buddy aid, medic, CBRN medical treatment) - Evacuation status: in place, being evacuated, evacuated to Role 2/3 - Decontaminated: Yes/No - Linked to CCP entry (if processed through CCP)

Coordinate with the battalion S1 and medical officer (surgeon) to ensure CBRN casualty data in MSS matches personnel and medical tracking data. Discrepancies indicate a reporting gap that must be resolved.

CHAPTER 4 — ANTITERRORISM AND FORCE PROTECTION

BLUF: The AT officer uses MSS to manage the full antiterrorism cycle: threat and vulnerability assessment data, FPCON levels, RAM scheduling and execution tracking, incident reporting, and AT lesson learned documentation. IAW ATP 3-37.2, AT is a continuous effort requiring current data — MSS provides the data infrastructure to sustain that currency.

4-1. AT Officer Workflow in MSS

The AT officer's MSS workflow follows the threat-assessment-countermeasure cycle: 1. Receive and load threat data from S2 and higher AT channels 2. Conduct/update vulnerability assessment data entries 3. Determine and load FPCON level (command-directed) 4. Build and maintain RAM schedule 5. Track RAM execution 6. Log AT incidents and near-misses 7. Document AT lessons learned

4-2. Threat and Vulnerability Assessment Data Management

TASK: Conduct and Document a Threat/Vulnerability Assessment in MSS

CONDITIONS: AT officer has received current threat assessment from S2 and higher AT authority. Unit facility or installation has been assigned for assessment. MSS AT workspace access is active.

STANDARDS: Assessment is documented in the MSS AT workspace using all mandatory data fields (see Appendix E). Vulnerability data is entered for all 18 CARVER + shock categories (ATP 3-37.2, para 2-4). Threat assessment source and date are documented. Approving authority (typically installation AT officer or commander) signs the assessment in MSS within 72 hours of entry. Assessment is reviewed and updated minimum every 180 days or after any significant threat change.

PROCEDURE: 1. Navigate to the AT Officer zone in the protection workspace. 2. Select "New Threat/Vulnerability Assessment." 3. Enter facility/installation identification data: name, grid, type (FOB, COP, transit point, facility), owning unit. 4. Enter threat assessment data: a. Threat source (specific group, generalized criminal threat, etc. — use S2 language) b. Threat category (direct attack, VBIED, indirect fire, insider threat, cyber/EW — as applicable) c. Threat probability (High, Medium, Low) with source and rationale d. Threat data source and date 5. Enter vulnerability data for each applicable CARVER + shock category. 6. Calculate overall vulnerability score. MSS displays the composite score automatically. 7. Determine threat × vulnerability = risk for each threat-vulnerability pair. 8. Document existing and planned countermeasures with responsible party and implementation status. 9. Submit to approving authority for electronic signature. 10. Link completed assessment to the AT officer's annual review schedule in MSS.

4-2a. CVP Analysis Framework — Driving Protection Priorities in MSS

Protection prioritization decisions depend on CVP analysis — Criticality, Vulnerability, Probability. ADP 3-37 (January 2024) establishes CVP as the framework by which commanders and protection cells determine which assets require the most protection. In MSS, CVP analysis provides the structured data foundation for producing the Critical Asset List (CAL) and the Defended Asset List (DAL).

Table 4-0. CVP Analysis Factors (IAW ADP 3-37)

Factor	Definition	Data Requirements
Criticality	How important is the asset to mission success?	Mission analysis, task organization, asset value
Vulnerability	How exposed is the asset to threats?	Threat assessment, terrain analysis, defensive posture
Probability	How likely is the threat to act against this asset?	Intelligence assessment, historical pattern data

CVP analysis is not a one-time event. The protection cell reviews CVP data at each Protection Working Group meeting and updates it after any significant change to the threat picture, the unit's defensive posture, or the mission. In MSS, CVP scores are attached to assets in the protection workspace and feed directly into CAL/DAL decisions (Chapter 6, para 6-4).

MSS CVP Data Entry: 1. Navigate to the AT Officer zone or protection workspace. 2. For each asset under consideration, enter Criticality, Vulnerability, and Probability scores using the standard High/Medium/Low scale. 3. Document the rationale and data source for each factor score. 4. MSS calculates the composite CVP risk score and ranks assets for prioritization. 5. The ranked list informs commander's CAL/DAL decisions and resource allocation for protection measures.

NOTE: CVP analysis produces the Critical Asset List (CAL) and Defended Asset List (DAL) — both are structured data products maintained in MSS. The CAL lists all assets requiring protection based on CVP scoring. The DAL is the subset of CAL assets that available AMD and protection resources can actively defend. The gap between CAL and DAL is accepted risk, which must be documented and briefed to the commander. See Chapter 6, para 6-4 for CAL/DAL management procedures.

WARNING: CVP scores are only as valid as the data feeding them. A Probability assessment based on 6-month-old threat data, or a Vulnerability assessment that does not account for a recent defensive posture change, produces a misleading protection priority list. The AT officer must verify data currency for all three CVP factors before presenting CVP-based recommendations to the commander.

4-3. FPCON Tracking and Communication in MSS

Force Protection Condition (FPCON) is the DOD-standardized system for managing and communicating terrorism threat levels. MSS tracks FPCON at unit and installation level with a full change log.

FPCON Levels:

Table 4-1. FPCON Levels and MSS Management (IAW ATP 3-37.2)

FPCON	Threat Level	Description	MSS Notification Trigger
NORMAL	No credible threat	Standard security posture	Baseline; no alert
ALPHA	General threat	Increased security awareness required	Alert to all units in workspace
BRAVO	Predictable threat	Increased specific security measures	Alert + measures checklist prompt
CHARLIE	Imminent threat	Implemented additional security measures	Alert + measures checklist + command notification
DELTA	Specific threat/attack	Maximum force protection posture	Alert + all cells + automatic PWG convene prompt

FPCON Change Procedure in MSS: 1. Receive command-directed FPCON change (through chain of command — NOT based on MSS alert alone). 2. Navigate to AT Officer zone. Select "FPCON Management." 3. Update current FPCON level for the unit/installation. 4. Enter change authority (name, position, DTG of direction). 5. Enter effective date/time. 6. Select notification recipients: all units in workspace, adjacent units, parent formation. 7. MSS logs the change with full attribution. Subordinate units in the shared workspace receive alert notification. 8. Access the FPCON measures checklist for the new level. Verify all required measures are assigned to responsible parties with completion tracking. 9. Report FPCON change IAW unit SOP (MSS change is the record; voice/SIPR reporting per SOP remains required).

CAUTION: FPCON in MSS reflects command-directed levels. Do NOT adjust FPCON in MSS based on an AT officer's independent assessment without command direction. FPCON is a command decision — it is not within the AT officer's unilateral authority to change.

4-4. Random Antiterrorism Measures (RAM) Management

RAM are measures implemented on a random, unpredictable schedule to deny adversaries the ability to conduct pattern analysis of unit security procedures. MSS provides a RAM scheduling, assignment, and execution tracking workspace.

RAM Management in MSS: 1. Navigate to the RAM workspace within the AT Officer zone. 2. Select RAM measures applicable to the current FPCON level from the AT-approved RAM menu. 3. Assign each RAM measure to a responsible position (not by name — by duty position to maintain continuity through personnel changes). 4. Set the randomized schedule: MSS provides a scheduler tool that generates random time windows within specified parameters. Do NOT create predictable patterns. 5. After each RAM execution window, the responsible position marks execution status: Executed, Not Executed (with reason), or Partially Executed. 6. Review RAM execution rate at the weekly Protection Working Group. RAM that is consistently not executed requires leader attention — not adjustment of the schedule to match what is actually being done.

NOTE: RAM effectiveness depends entirely on unpredictability. Do not share the RAM schedule with personnel not required to execute those measures. Coordinate with OPSEC officer on RAM schedule handling. The RAM schedule in MSS should be protected at the appropriate classification level.

4-4a. Conducting a RAM Schedule Review in MSS

TASK: Conduct a Weekly RAM Execution Review in MSS

CONDITIONS: The AT officer or protection officer is preparing for the Protection Working Group. One week of RAM execution data is available in the MSS AT zone. Current RAM schedule is loaded.

STANDARDS: The RAM execution review identifies the percentage of scheduled RAM measures executed, any RAM windows that were not executed with documented reasons, and any patterns of non-execution that indicate systemic RAM compliance problems. Results are briefed at the PWG. RAM measures consistently not executed for non-operational reasons are escalated to the commander.

PROCEDURE: 1. Navigate to the AT Officer zone. Select "RAM Execution Review." 2. Set the review period to the past 7 days. 3. Export or view the RAM execution summary: - Total RAM windows scheduled in the period - Total executed (marked "Executed" by responsible position) - Total not executed (marked "Not Executed" with reason) - Total partially executed 4. Calculate the execution rate: (Executed ÷ Total Scheduled) × 100. 5. Review the "Not Executed" entries. Reasons are categorized: - Operational (unit deployed, no available personnel — acceptable) - Resource (equipment unavailable — requires corrective action) - Planning (RAM window scheduled when execution was not feasible — scheduling issue) - No reason entered (requires immediate follow-up — data entry failure) 6. Identify any RAM measures that have not been executed in two consecutive windows with non-operational reasons. Flag for commander attention. 7. Identify any predictable pattern in execution timing (e.g., RAM is always executed at the same time within the window). Flag this as a RAM effectiveness issue — the measure is being scheduled randomly but executed predictably. 8. Prepare the RAM execution brief for the PWG: execution rate, non-execution reasons, patterns identified, corrective actions recommended.

NOTE: A RAM execution rate below 85% (excluding operationally-justified non-executions) indicates an AT program compliance problem. A RAM execution rate of 100% that shows a consistent time pattern also indicates a problem — RAM is only effective when it is genuinely unpredictable.

4-5. Incident Reporting and AT Lessons Learned

AT incident data in MSS provides the raw material for lessons learned and trend analysis. Every AT-relevant incident — from gate runners to IED finds — is logged in the AT incident workspace.

AT Incident Data Fields: - Incident type (gate runner, perimeter breach, VBIED, IED find, suspicious activity, insider threat indicator, near-miss) - Date-time group (DTG) - Location (grid) - Description (narrative, factual — not analytical) - Response taken - Outcome - Linked to FPCON level at time of incident - Lessons learned (documented after incident review) - Status: Open (under investigation), Closed (resolved), Referred (forwarded to CID/higher AT authority)

Coordinate with 31D (CID) for incidents that meet the threshold for criminal investigation referral. CID maintains a parallel investigation record; AT incident data in MSS is the protection cell's operational record, not the official investigative record.

4-6. MISO and PSYOP Coordination with the AT Officer in MSS

Psychological Operations (37F) and the AT officer coordinate in the force protection domain when MISO activities support AT objectives — primarily in the areas of threat deterrence, suspicious activity reporting campaigns, and deception as a force protection measure. In MSS, this coordination is documented in the AT workspace.

37F MSS Data Responsibilities in the Protection Context:

MISO personnel do not manage the AT workspace. Their role is to provide data from MISO activities that is relevant to the AT officer's threat picture, and to receive AT threat data that informs MISO product development for force protection purposes.

MISO data contributed to the AT workspace: - Reports from local national interaction that indicate threat actor interest in the installation (crowd activities, pattern changes near ECPs, unexplained photography) - Information from MISO operations that reveals potential insider threat indicators - Assessment of local information environment: is the threat messaging environment escalating or de-escalating?

AT data received by MISO from MSS: - Current FPCON level (informs tone and urgency of any force protection MISO products) - AT incident data summary (what threat activities have occurred — informs MISO product relevance) - Approved threat messaging guidance (informs MISO products that support force protection)

Coordination Procedure: 1. The AT officer designates which AT workspace data elements are shareable with the MISO team. Not all AT data is appropriate for MISO access — particularly sources and methods for threat intelligence. 2. MISO team lead coordinates with AT officer weekly to exchange relevant data. 3. MISO team enters force-protection-relevant field observations in the AT incident workspace as "MISO Field Report" entries — distinguished from AT incident reports. 4. AT officer reviews MISO entries before incorporating them into the threat assessment. MISO field observations are "Suspected" confidence by default — they require AT officer and S2 correlation before elevation to "Probable" or "Confirmed."

NOTE: MISO personnel are force protection multipliers, not AT officers. Their value to the AT program is in the texture of the human information environment they observe during MISO activities. The AT officer remains responsible for threat assessment and protective action decisions.

4-7. OPSEC 5-Step Process as a Data Security Framework

Operations Security (OPSEC) is a protection task that applies across the entire force — not just within the AT cell. FM 3-13.3 establishes the 5-step OPSEC process. For MSS practitioners, the OPSEC process maps directly to data security practices on the platform. Every protection data element managed in MSS is potential intelligence for an adversary; OPSEC discipline determines whether MSS data exposure is controlled.

Table 4-2. OPSEC 5-Step Process and MSS Data Platform Analog (IAW FM 3-13.3)

Step	OPSEC Action	Data Platform Analog
1	Identify critical information	Define sensitive data elements, classification rules
2	Analyze threats	Threat intelligence feeds, adversary collection capability assessment
3	Analyze vulnerabilities	Access audit, data exposure analysis, metadata review
4	Assess risk	Risk scoring, residual risk acceptance
5	Apply countermeasures	Access controls, data masking, need-to-know enforcement

Applying the OPSEC Process to MSS Protection Data:

1. **Identify critical information.** The unit OPSEC officer and protection cell identify which protection data elements in MSS constitute critical information — data that, if obtained by an adversary, would compromise operational security. Examples: RAM schedule, specific FPCON measures, vulnerability assessment scores for specific facilities, AMD system locations and readiness states.
2. **Analyze threats.** Determine which adversary collection capabilities could target MSS data. This includes insider threat, cyber exploitation, and observation of MSS terminals during field operations. Coordinate with S2 for current adversary collection capability assessments.
3. **Analyze vulnerabilities.** Conduct an access audit of the protection workspace. Who has access to which data zones? Are access permissions current, or do departed personnel still have active permissions? Is metadata (timestamps, editor names, change logs) exposing patterns that reveal operational information?
4. **Assess risk.** Score the risk of each critical information element being compromised. Risk = Threat × Vulnerability. Document risk scores in the OPSEC risk workspace linked to the protection workspace.
5. **Apply countermeasures.** Implement data-level countermeasures in MSS: restrict workspace access to need-to-know, apply data masking for sensitive fields visible in shared views, enforce classification markings on all protection data products, and conduct periodic access reviews.

NOTE: OPSEC is not an IT function — it is a commander's program executed by all staff. The OPSEC officer coordinates and advises, but every protection practitioner who enters data in MSS is responsible for understanding what constitutes critical information and how to protect it on the platform. AR 530-1 and ATP 3-13.3 provide the regulatory and doctrinal framework.

CAUTION: MSS metadata — who accessed a record, when, how frequently — can itself be critical information. An adversary who observes a sudden increase in AT workspace activity can infer a change in the threat posture. Coordinate with the OPSEC officer on metadata exposure risks specific to MSS usage patterns.

CHAPTER 5 — PHYSICAL SECURITY AND ACCESS CONTROL

BLUF: Military Police (31A officers, 31B soldiers) use MSS to manage access control data, perimeter visualization, guard scheduling, and incident reporting. MSS integrates physical security data with the broader force protection picture — connecting what happens at the gate to the overall AT risk picture.

5-1. MP Officer and Soldier Workflow in MSS

31A (MP Officer) Responsibilities in MSS: - Manage the physical security data layer for the installation or base camp - Maintain ECP data and status - Coordinate with AT officer on access control measures linked to FPCON levels - Review and approve SIR data entries before submission up the reporting chain

31B (Military Police) Responsibilities in MSS: - Enter incident reports during or immediately after shift - Update ECP status at shift change - Log gate runner events, suspicious vehicles/persons, access denials - Maintain duty log data for the shift

5-2. Entry Control Point Data Management

TASK: Manage Entry Control Point (ECP) Data in MSS

CONDITIONS: Unit is operating a base camp or installation with one or more ECPs. MP unit has MSS access. Physical security plan is established and approved.

STANDARDS: All active ECPs are entered in the MSS physical security workspace with complete data fields. ECP status is updated at each shift change (minimum every 8 hours). Gate incidents are entered within 30 minutes of occurrence. ECP data accurately reflects current access control posture for the installation.

PROCEDURE: 1. Navigate to the PMO zone within the unit protection workspace. 2. Select "ECP Management." 3. For each ECP, verify or enter: a. ECP designation (ECP 1, ECP 2, etc.) and name/callsign b. Location (8-digit grid) c. Operational status: Open, Restricted (limited access hours), Closed d. Access category: All personnel, Credentialed only, Military only, Escort required e. Guard post assignment (duty position, not name) f. Current FPCON measures in effect at this ECP g. Vehicle inspection status: Search in effect, Visual only, No search 4. At shift change, the incoming guard commander verifies all ECP entries and updates status. 5. Any change to ECP status (closing, restricting access, adding search requirement) is entered in MSS with DTG and authority for the change. 6. All ECPs are visible on the geospatial base camp layer in MSS. Confirm plot accuracy against physical positions.

5-3. Base Perimeter Visualization and Access Layer Management

The MSS physical security geospatial layer displays the installation or base camp perimeter as a data layer, integrated with the broader protection operating picture. This layer includes: - Perimeter trace (drawn from actual survey/site data, not from memory) - ECP locations and status (color-coded: green = open, amber = restricted, red = closed) - Guard post locations (interior and perimeter positions) - Access control zones (unrestricted, restricted, exclusion zone) - Dead ground and observation gaps (identified through physical reconnaissance and entered as data) - Camera coverage overlays (if applicable) - Barrier and obstacle features (jersey barriers, HESCO, concertina wire)

The perimeter visualization layer is maintained by the PMO and reviewed at the Protection Working Group. Changes to the physical perimeter require an update to the MSS layer within 24 hours.

5-4. Guard Schedule and Post Data Tracking

Guard schedule data in MSS provides visibility on guard force disposition and enables the PMO to identify coverage gaps before they occur.

Guard Schedule Data Fields: - Posting name and number (Post 1, Main Gate, Tower Alpha, etc.) - Relief schedule (start DTG, duration, relief DTG) - Required personnel strength for each post - Actual assigned strength - Armed/unarmed status - Rules of engagement (ROE) summary or reference (not full text — reference the current ROE card) - Supervisor for shift

MSS does not manage individual personnel scheduling at the level of naming which Soldier is on which post — that remains a unit function managed through the S1/HR system. MSS tracks post data and coverage status, not individual assignments.

5-5. Incident and Serious Incident Report (SIR) Tracking

TASK: Enter and Track a Serious Incident Report (SIR) in MSS

CONDITIONS: A reportable incident has occurred at or near the installation. The MP desk officer or duty officer has determined the incident meets SIR criteria. MSS PMO workspace access is active.

STANDARDS: SIR data is entered in MSS within 1 hour of the incident being identified as SIR-reportable. All mandatory data fields are complete before submission up the reporting chain. SIR is linked to the relevant ECP or location in the geospatial layer. Status is updated at each significant development until the incident is closed.

PROCEDURE: 1. Navigate to PMO zone. Select "Incident/SIR Tracking." 2. Select "New SIR Entry." 3. Enter incident category (IAW AR 190-40 SIR category list). 4. Enter incident data: a. DTG of incident (not DTG of report entry) b. Location (grid and description) c. Unit(s) involved d. Description of incident (factual narrative — who, what, when, where; no speculation) e. Actions taken f. Current status 5. Assign

classification level appropriate to the incident content. 6. Link to associated ECP, guard post, or location marker in the geospatial layer. 7. Submit for PMO officer review and approval before upward reporting. 8. After command review, enter the formal SIR reference number received from higher. 9. Update status as investigation or response actions develop.

5-5a. Conducting a Physical Security Inspection and Entering Findings in MSS

TASK: Conduct a Physical Security Inspection and Document Findings in MSS

CONDITIONS: The PMO or AT officer has scheduled a physical security inspection of the installation or base camp IAW the unit inspection schedule or FPCON requirements. MSS PMO workspace access is active. The current security plan data is accessible.

STANDARDS: All inspection findings — both deficiencies and compliant areas — are entered in the MSS physical security inspection record within 24 hours of inspection completion. Deficiencies are assigned a severity rating and a corrective action with responsible party and deadline. Repeat deficiencies from prior inspections are flagged as systemic issues. Inspection record is linked to the relevant ECP, guard post, or facility in the geospatial layer.

PROCEDURE: 1. Navigate to the PMO zone. Select "Security Inspections." 2. Select "New Inspection Record." 3. Enter inspection type: Routine, FPCON-Directed, Command-Directed, Post-Incident. 4. Enter inspection scope: ECP Only, Full Perimeter, Facility-Specific, All. 5. Enter inspector name(s) and rank/position. 6. For each area inspected, enter: a. Area name/description and grid b. Finding type: Compliant, Minor Deficiency, Major Deficiency, Critical Deficiency c. Deficiency description (specific — "Gate 2 vehicle barrier is retracted and unattended, 1425 hours 12 MAR 26" not "gate barrier not in use") d. Applicable security standard violated (AR 190-13 paragraph, unit SOP section, or FPCON measure) e. Recommended corrective action f. Responsible party for correction (duty position) g. Deadline for corrective action (based on deficiency severity: Critical = 24 hours, Major = 72 hours, Minor = 7 days) 7. Check each finding against prior inspection records for the same area. Mark any deficiency that appeared in the prior inspection as a "Repeat Finding" — this automatically flags it for commander attention. 8. Submit inspection record to PMO officer for review and approval. 9. PMO officer assigns corrective actions and notifies responsible parties through MSS task function. 10. Track corrective action completion: responsible party marks action complete in MSS. PMO officer verifies completion on next inspection.

5-6. Installation Security Plan Data Management

The Installation Security Plan (or Base Defense Plan) is a living document. MSS supports maintenance of the data elements of the plan as a structured data layer, separate from the formal document itself.

Security Plan Data Elements in MSS: - Threat assessment data (linked to AT workspace entry) - FPCON measures by level (linked to AT officer zone) - ECP data (linked to physical security layer) - Guard force summary (headcount by post category) - Emergency response plans: reference links, not full text in MSS - QRF data: location, strength, response time, alert procedures - Access control waiver register (personnel with special access authority) - Security inspection schedule and last inspection date

CHAPTER 6 — AIR AND MISSILE DEFENSE (PROTECTION ASPECT)

BLUF: AMD contributes to the protection WFF through management of the air threat picture, critical asset/defended asset list management, and coordination of AMD coverage with maneuver forces. ADA officers (14A) and operators (14E, 14P, 14S) use MSS to maintain AMD data and coordinate with the fires WFF. Cross-reference SL 4B (Fires) for AMD coordination from the Fires perspective.

6-1. AMD's Role in the Protection WFF

Air and missile defense is a protection function — it protects forces and critical assets from aerial threats. IAW ADP 3-37, AMD is one of the protection tasks that commanders integrate into the overall protection scheme. At the same time, AMD is inherently coordinated with the fires WFF (airspace management, engagement coordination, ROE). MSS provides a common operating platform where protection data and fires data intersect for AMD.

The AMD cell's data responsibilities in MSS: - Maintain the air threat picture and ADW status - Manage the CAL/DAL - Track AMD system readiness and employment status - Coordinate engagement areas and sectors with maneuver and fires elements - Record AMD engagements as data entries for reporting and post-engagement analysis

6-2. Air Threat Picture Visualization in MSS

The MSS AMD workspace displays the air picture as a geospatial data layer integrated with other protection and fires data. Data for the air picture comes from AMD system feeds (where interfaced), ADAM/BAE cells, and manual entry.

Air Picture Data Layers in MSS: - AMD system locations (Patriot, SHORAD, Avenger, Stinger teams) — plotted as geospatial objects with status - AMD engagement zones (high-altitude, medium-altitude, SHORAD, gun target line data) - Air corridors (coordinating measures: ACMs, ALTRVs, restricted operations zones) - Threat tracks (fed from higher AMD nets or entered manually from voice reports) - THAAD/Patriot interceptor status (for theater AMD elements)

NOTE: The MSS air picture for AMD purposes represents a planning and tracking layer — it is NOT a replacement for actual radar data, IBCS data, or AMD battle management systems. Track correlation and engagement decisions occur in AMD-specific battle management systems. MSS provides the operational-level picture for the protection and fires staff.

6-3. Air Defense Warning Tracking

Air Defense Warning (ADW) is the standardized system for communicating air threat levels (WHITE, YELLOW, RED). MSS tracks current ADW for the unit's AOR and logs changes with attribution.

ADW Management in MSS: 1. Navigate to AMD zone in protection workspace. 2. Select "ADW Status." 3. Current ADW displays with source (AAMDC, theater AMD authority) and effective time. 4. To update ADW: enter new warning color, directing authority, DTG of direction, and effective time. 5. MSS sends alert notification to all units in shared workspace when ADW changes to YELLOW or RED. 6. ADW change log is maintained automatically — do not delete or edit past entries.

6-4. Critical Asset List / Defended Asset List Management

The CAL identifies assets critical to the mission that require protection from air and missile threats. The DAL is the subset of CAL assets that AMD assets will actively defend given available resources. The gap between CAL and DAL represents accepted risk — a command decision (FM 3-01, para 2-3).

TASK: Maintain the Critical Asset List (CAL) and Defended Asset List (DAL) in MSS

CONDITIONS: The G3/S3 and AMD officer have received CAL/DAL guidance from the commander. AMD workspace access is active. Mission asset data is available.

STANDARDS: All CAL assets are entered in the MSS AMD workspace with complete data fields. DAL designation is current and reflects commander-approved AMD coverage. CAL/DAL data is reviewed and updated minimum every 30 days or after any significant mission change.

PROCEDURE: 1. Navigate to AMD zone. Select "CAL/DAL Management." 2. For each critical asset, enter: a. Asset name and type (command post, logistics node, communications site, key bridge, airfield, etc.) b. Grid location c. Priority (I, II, III — based on mission criticality) d. CAL designation: Yes/No e. DAL designation: Yes/No (command decision based on AMD resource availability) f. Justification for CAL/DAL designation g. Supporting commander or authority who directed the designation 3. Plot each CAL/DAL asset on the AMD geospatial layer. 4. For DAL assets, link to the AMD system assigned to defend that asset. 5. Identify CAL assets NOT on the DAL — these represent accepted air/missile risk. Document accepted risk rationale. 6. Brief CAL/DAL status at the Protection Working Group. Changes to the DAL require commander approval.

6-4a. AMD System Employment Status Tracking

The ADA officer tracks AMD system employment status in MSS to maintain visibility on the AMD coverage picture across the AOR. This data drives the CAL/DAL review — if a system that was providing coverage to a DAL asset is NMC, the protection picture changes and the commander must be informed.

TASK: Maintain AMD System Employment Status in MSS

CONDITIONS: ADA battery or SHORAD element is deployed and operational. AMD workspace access is active. System locations, sectors, and readiness data are known.

STANDARDS: All deployed AMD systems are entered in the MSS AMD workspace with complete employment status data. Status is updated within 30 minutes of any change to FMC/PMC/NMC status. System relocation is updated within 1 hour of completing displacement. Coverage gap analysis is updated within 2 hours of any system going NMC.

PROCEDURE: 1. Navigate to AMD zone. Select "AMD System Status." 2. For each deployed AMD system, verify or enter: a. System type: Patriot, THAAD, SHORAD (Avenger, Stinger team, SHORAD type), Air Defense Sentinel radar b. Assigned unit and callsign c. Grid location (current — update on displacement) d. FMC/PMC/NMC status e. Ammunition load: status (full, partial — quantity, expended — requires resupply) f. Sector of fire: azimuth limits and altitude envelope (for SHORAD) g. Engagement status: Weapons Free, Weapons Tight, Weapons Hold (per current ROE and AMD ROE) h. Last maintenance date and next scheduled maintenance 3. For NMC systems, enter estimated return-to-FMC date and reason (maintenance, supply, battle damage). 4. Link each system to the CAL/DAL assets it provides coverage for. When a system goes NMC, MSS displays a coverage gap alert for the linked DAL assets. 5. Brief AMD system status at the Protection Working Group. Coverage gaps are a protection risk item — commanders need to know what CAL assets are temporarily undefended.

6-5. AMD-Maneuver Deconfliction Data

AMD systems operating near maneuver forces require deconfliction to prevent fratricide. MSS tracks AMD employment constraints and coordinates with the airspace management workspace (typically an S3 Air or ADAM/BAE function).

AMD Deconfliction Data in MSS: - AMD unit locations (plotted for maneuver element awareness) - Engagement zones (defined by altitude and geographic boundary) - Friendly aircraft routes through AMD engagement zones (coordination measures) - ROE constraints data (applicable AMD ROE in effect, by zone) - Communication frequencies for AMD-maneuver coordination

---

6-6. Counterintelligence Support to Protection — 311A/311B Role in MSS

Counterintelligence (CI) agents and warrant officers (311A/311B) support the protection WFF through insider threat detection, force protection intelligence, and AT-relevant reporting. In MSS, CI personnel work primarily through the AT officer zone, coordinating data that informs the threat picture without exposing sources and methods.

CI Data Contributions to the MSS Protection Workspace:

CI does not manage the protection workspace independently. The 311A/311B CI element provides data to the AT officer and S2 that enriches the protection threat picture. The AT officer incorporates this data into the AT assessment, with source protection maintained per CI handling requirements.

Force Protection Relevant Reporting: - Information about threat actor reconnaissance activities targeting installations or personnel - Insider threat indicators (behavioral, access-related, pattern deviations) that do not yet meet the threshold for formal investigation - Assessments of foreign intelligence service interest in USAREUR-AF personnel or activities

MSS Entry Procedure for CI-Relevant AT Data: 1. CI special agent coordinates with the AT officer on what data can be entered in MSS and at what classification level. 2. CI-relevant AT entries are labeled "Source: CI Element" with no further source attribution in the MSS record. 3. AT officer maintains a separate coordination record (not in MSS) that links the CI report to the MSS entry for traceability within appropriate channels. 4. CI-relevant entries are marked with a "Restricted Distribution" flag in MSS — visible only to AT officer, S2, and commander. Not distributed to the full protection workspace.

CAUTION: CI sources and methods are among the most sensitive data in the protection picture. Never enter specific CI source descriptions, collection methods, or investigation subjects in the MSS protection workspace. MSS is not an appropriate system for storing CI investigative data. Coordinate with the 311A/S2X for appropriate handling of CI-derived protection data.

CHAPTER 7 — ELECTRONIC WARFARE AND SPECTRUM MANAGEMENT

BLUF: EW functions as a protection enabler by denying adversaries the ability to detect, locate, or disrupt friendly forces through the electromagnetic spectrum. MSS supports EW as a protection function through spectrum management data, jamming threat reporting, and counter-UAS tracking. Cross-reference the S6 (SL 4F sections on signal) and the fires WFF for EW attack functions.

7-1. EW as a Protection Enabler

IAW FM 3-36, electronic warfare consists of electronic attack (EA), electronic protection (EP), and electronic support (ES). In the protection WFF context, EW supports protection through: - Electronic protection: maintaining friendly use of the EM spectrum against adversary jamming or exploitation -

Electronic support: identifying adversary emission sources that represent threat indicators - Counter-UAS: electronic defeat of hostile UAS through jamming or spoofing (coordination with AMD and legal)

MSS does not replace EW-specific systems (JCREW, THOR, DUKE, CREW systems). MSS tracks EW as a data domain — managing reports, incidents, spectrum allocation, and counter-UAS data — to integrate EW information into the protection and operations picture.

7-2. Spectrum Management in MSS

Frequency allocation data in MSS provides visibility on the unit's allocated frequencies, potential interference sources, and spectrum coordination actions. This is primarily an S6 function, but the protection cell has an interest in spectrum data as it relates to EW threat identification and counter-UAS operations.

Spectrum Management Data in MSS: - Allocated frequencies by system and unit (reference only — full JFMO data resides in separate spectrum management systems) - Frequency interference reports (source, affected system, DTG, location) - Interference resolution status - Restricted frequency bands (from JFMO or corps/theater direction) - Counter-UAS frequency coordination data (if applicable)

7-3. Jamming Threat Reporting and EW Incident Data

TASK: Enter and Track a Jamming or EW Incident in MSS

CONDITIONS: Unit has identified or confirmed jamming, spoofing, or other EW interference affecting operations. The S6 and EW officer have been notified. EW incident data is available.

STANDARDS: EW incident data is entered in the MSS EW tracking workspace within 30 minutes of incident identification. All mandatory data fields are complete. Incident is linked to the affected system(s) in the spectrum management data layer. Incident status is updated until resolution. Reported IAW unit SOP and higher EW reporting requirements.

PROCEDURE: 1. Navigate to the EW zone within the protection or operations workspace (unit-specific — coordinate with S6 for workspace location). 2. Select "New EW Incident." 3. Enter incident type: Jamming, Spoofing, Exploitation suspected, Electronic deception. 4. Enter affected system(s) and frequency or band. 5. Enter location of incident and direction of interference source (if determinable from bearing data or other analysis). 6. Enter DTG of first detection. 7. Describe operational impact: Communications degraded, GPS unreliable, system offline, navigation affected. 8. Enter actions taken: frequency change, system reconfiguration, reported to higher, counter-jamming measures employed. 9. Report through EW reporting chain IAW unit SOP. MSS entry is the unit record — voice/digital reporting up the chain is still required.

7-4. Counter-UAS Operations Data in MSS

Counter-UAS (C-UAS) is an emerging protection task with a significant data management requirement. UAS threats are detected, identified, and defeated through multiple means — electronic, kinetic, and directed energy. MSS tracks C-UAS operations data to build the unit's C-UAS picture and support reporting.

C-UAS Data Domains in MSS:

Phase	Data Tracked	Entry Responsibility
Detect	UAS detection event, sensor type, grid, DTG, altitude/heading if known	Air Defense/Counter-UAS NCO
Identify	UAS classification (Group 1–5, friendly/adversary/unknown), identification method	AMD officer or S2 with AMD coordination
Defeat	Defeat method (EW, kinetic, directed energy), result (defeated, evaded, lost track), DTG	AMD officer or EW officer
Report	Post-event report to higher, linked to detection and defeat entries	AT officer or AMD officer

WARNING: Engagement of UAS systems with kinetic or electronic means requires engagement authority confirmation IAW applicable theater ROE and ATP 3-01.81. Do NOT initiate defeat actions based on MSS tracking data alone. MSS documents what occurred — it does not grant engagement authority.

7-4a. Managing Counter-UAS Reporting in MSS

TASK: Enter and Track a UAS Detection-to-Defeat Event in MSS

CONDITIONS: A UAS has been detected within or approaching the unit's AOR. The AMD officer or Counter-UAS team has initiated the detect-identify-defeat sequence. C-UAS workspace access is active in MSS.

STANDARDS: Detection event is entered in MSS within 5 minutes of first detection. Identification assessment is entered as soon as assessed — not delayed pending confirmation. Defeat action is entered within 15 minutes of action initiation. Post-event record is complete within 2 hours of event conclusion. All entries use the UAS track naming convention (see Appendix A). Engagement authority is documented for all defeat actions.

PROCEDURE: Phase 1 — Detection Entry: 1. Navigate to C-UAS zone in protection workspace. 2. Select "New UAS Detection Event." 3. Enter detection DTG (time of first detection, not time of entry). 4. Enter detection sensor/method: visual, acoustic sensor, radar, EO/IR, RF direction finding, other. 5. Enter

initial track data: grid of detection, altitude estimate if known, azimuth/bearing from detection sensor. 6. Enter initial classification: Known Friendly, Suspected Hostile, Unknown. Mark as "Unknown" if classification is not yet determined — do not assume. 7. Check for existing tracks in MSS for the current area. If a track exists that could be the same object, link this detection to the existing track rather than creating a new entry. This is the track correlation step. 8. Assign UAS track identifier per naming convention.

Phase 2 — Identification Entry: 9. As identification data develops, update the track classification. Document the identification basis: - RF signature match to known threat UAS - Visual identification of UAS type - Flight pattern analysis - Correlation with reported threat activity 10. Update classification: Confirmed Friendly (stop defeat actions), Probable Hostile, Confirmed Hostile. 11. For Probable or Confirmed Hostile: notify AMD officer and confirm engagement authority status.

Phase 3 — Defeat Action Entry: 12. If defeat action is authorized, enter defeat method: Electronic Warfare (jamming/spoofing), Kinetic (direct fire or interceptor), Directed Energy. 13. Enter engagement authority: name, position, DTG of authorization. 14. Enter result: Neutralized, Forced Landing, Track Lost, No Effect Observed, Friendly/Civilian (abort — document engagement abort and reason). 15. For kinetic or directed energy defeat: enter approximate impact location if observable.

Phase 4 — Post-Event Record: 16. Enter lessons learned: Was the detection-to-defeat sequence within standard time? Were there identification challenges? Did coordination work as planned? 17. Submit post-event record to AMD officer and AT officer for review. 18. Link to any associated EW incident report if frequency interference was involved in the defeat method.

WARNING: Any UAS defeat action that is subsequently assessed as engagement of a civilian or friendly UAS must be reported immediately through the chain of command and documented in MSS with full engagement authority attribution. Do not delay reporting or edit entries to obscure the sequence of events. The MSS record is the unit's official event record.

7-5. Frequency Interference Reporting

Frequency interference that is not jamming (i.e., unintentional interference from friendly or civilian sources) is tracked separately from EW incidents. MSS maintains a frequency interference log that S6 and EW elements use for spectrum deconfliction.

Interference Report Data Fields: - Affected unit and system - Frequency/band affected - Nature of interference: adjacent channel, intermodulation, spurious emission - Suspected source (if known) - Impact on operations - Actions taken and resolution status

---

CHAPTER 8 — SURVIVABILITY OPERATIONS

BLUF: Combat engineers (12B) and base camp planners use MSS to manage survivability position data, facility hardening status, camouflage and concealment planning, and base camp design data. MSS integrates survivability data into the protection picture to enable commanders to assess defensive posture across the AOR.

8-1. ATP 3-37.34 Survivability Planning in MSS

Survivability operations reduce the vulnerability of personnel, weapons, and equipment to enemy attack and environmental hazards (ATP 3-37.34, para 1-1). In MSS, survivability planning data is maintained as a distinct layer within the protection workspace, managed by the engineer cell with protection officer visibility.

Survivability data categories in MSS: 1. Fighting positions and survivability positions (location, status, construction standard) 2. Facility hardening status (key structures, command posts, communications sites) 3. Camouflage, concealment, and decoy (CCD) planning data 4. Obstacle and barrier data (integrated with base camp design) 5. Base camp design data (IAW ATP 3-37.10)

8-1a. Survivability Planning and MSS — The Engineer-Protection Interface

Survivability operations sit at the interface between the engineer corps and the protection WFF. The combat engineer (12B) plans and constructs survivability positions; the protection officer ensures those positions are tracked and integrated into the protection picture. In MSS, this interface is managed through the survivability zone of the protection workspace.

The engineer section should not manage survivability data in isolation. The protection officer needs visibility on survivability status — where positions are, what standard they are built to, what gaps exist — to advise the commander on the unit's defensive posture. A fighting position that is constructed but not entered in MSS is invisible to the protection picture and cannot inform planning.

Engineer-Protection Data Handoff Points: - When positions are planned: Engineer enters planned positions in MSS so the protection officer can identify coverage gaps before construction begins. - When construction begins: Status updates to "Under Construction" with materials on hand and estimated completion. - When construction is complete: Status updates to "Complete" with construction standard verified. - When positions are damaged: Status updates to "Damaged" within 24 hours of damage assessment, with repair priority assigned. - When positions are abandoned: Status updates to "Closed" when the unit displaces from that position.

The engineer section's primary MSS value in the protection WFF is the quality and currency of position data. A map that shows planned positions as "complete" when they are still under construction — or completed positions as "planned" because the update was never entered — produces a false confidence

in the unit's defensive posture.

NOTE: The engineer section is the data entry authority for survivability positions. The protection officer is the data quality authority — verifying during the weekly review that survivability data reflects the physical reality of the AO. These are complementary, not competing, roles.

NOTE: The FM 3-34 (Geospatial Engineering) GMAD framework — Generate, Manage, Analyze, Disseminate — maps directly to the MSS data pipeline for protection geospatial products. Generate = ingest geospatial data (terrain, threat overlays, position data). Manage = govern data quality, classification, access. Analyze = transform raw geospatial data into protection overlays and threat mapping products. Disseminate = publish finished geospatial products to subordinate units and adjacent WFFs. Protection overlays, threat mapping, survivability position layers, and base camp design data in MSS all follow the GMAD-to-Ingest-Govern-Transform-Publish pipeline. Engineer sections and protection cells that understand this analog can apply FM 3-34 geospatial discipline to their MSS data management practices.

8-2. Fighting Position and Survivability Position Tracking

TASK: Enter and Track Fighting/Survivability Position Data in MSS

CONDITIONS: Unit is in a defensive or semi-permanent position. Engineer section has conducted survivability position reconnaissance and planning. Survivability workspace access is active in MSS.

STANDARDS: All planned and constructed fighting positions are entered in the MSS survivability layer within 24 hours of construction beginning. Each entry includes position type, grid, construction standard, status, and assigned element. Position status is updated within 24 hours of any change (completed, reinforced, damaged, abandoned).

PROCEDURE: 1. Navigate to the survivability zone in the unit protection workspace. 2. Select "New Survivability Position." 3. Enter position type: - Fighting Position (infantry, crew-served weapon, vehicle) - Command Post Position (CP hardening) - Logistics Area Position - Observation Post - Communications Site Protection 4. Enter position grid (8-digit). 5. Enter construction standard: Hasty, Improved, Deliberate (IAW FM 5-34 standards). 6. Enter assigned element (company, platoon, section — duty position, not individual names). 7. Enter construction status: Planned, Under Construction, Complete, Reinforcement in progress. 8. Plot on the survivability geospatial layer. 9. Link to the base camp design data layer if the position is part of a deliberate base camp. 10. Update status at each PWG or when physical status changes.

8-3. Hardening Status for Key Facilities

Key facilities require hardening assessment data separate from fighting positions. Command posts, communications sites, and logistics nodes are priority hardening targets.

Facility Hardening Data Fields: - Facility name and designation - Grid location - Facility type (CP, comms site, medical facility, motor pool, fuel point, ammunition supply point) - Current hardening level: None, Partial (sandbags/HESCO on one or two sides), Substantial (three sides + overhead cover), Full (360° + overhead + hardened access) - Priority for additional hardening (command directed) - Hardening materials requested vs. on hand - Responsible engineer element and completion estimate - Last inspection date

The protection officer reviews facility hardening status at the PWG. Facilities below required hardening standard are flagged as survivability risk items requiring command attention.

8-4. Camouflage, Concealment, and Decoy Planning Data

CCD planning data in MSS tracks the unit's camouflage and concealment plan as a data layer. This is primarily used to verify that CCD measures are implemented consistently across the AOR and to identify positions that lack adequate concealment from aerial observation.

CCD Data Fields: - Position or facility covered by the CCD plan entry - CCD measures in place: natural vegetation, camouflage nets, decoy positions, thermal masking - Aerial observation assessment (assessed from map and imagery, not live observation — update with actual assessment data) - Last CCD inspection date - Deficiencies identified and corrective actions assigned

8-4a. Conducting a Survivability Assessment and Documenting Deficiencies in MSS

TASK: Conduct a Survivability Assessment and Enter Deficiencies in MSS

CONDITIONS: The commander or protection officer has directed a survivability assessment of the current AO. The engineer section has conducted physical reconnaissance of positions, facilities, and the base camp perimeter. Survivability workspace access is active in MSS.

STANDARDS: All survivability deficiencies identified during reconnaissance are entered in the MSS survivability layer within 24 hours of completing the assessment. Each deficiency includes: location, deficiency type, severity rating, recommended remediation, engineer resources required, and priority (command-directed). Deficiencies are linked to the corresponding position or facility entry in the survivability geospatial layer.

PROCEDURE: 1. Navigate to survivability zone. Select "Survivability Assessment." 2. Enter assessment date and lead engineer (name and position). 3. For each position or facility assessed, review the existing MSS entry. Verify the entry is current and accurate before adding deficiency data. 4. For each deficiency

identified, select "Add Deficiency" from the position's record. 5. Enter deficiency type: - Construction Standard (position does not meet required standard for its designation: hasty vs. deliberate) - Overhead Cover (fighting position or facility lacks required overhead protection) - Standoff Violation (position or facility is within minimum standoff distance from perimeter wire) - CCD Deficiency (position is visually exposed from likely aerial or ground observation angles) - Drainage (position is subject to flooding — reduces fighting effectiveness and causes equipment damage) - Electrical/Utility (facility hardening does not account for utility entry points) - Obstacle Gap (perimeter has a gap in barrier obstacle allowing direct vehicle or dismounted access) 6. Enter severity: Minor (does not significantly degrade protection), Moderate (reduces protection capability), Critical (position/facility provides inadequate protection — likely casualty producer if targeted). 7. Enter remediation: materials required, labor estimate, engineer equipment required. 8. Enter priority: 1 (address within 24 hours), 2 (address within 72 hours), 3 (address within 7 days). 9. Link deficiency to the position's geospatial marker. 10. After all deficiencies are entered, generate the survivability assessment summary and brief to the commander. Assign corrective actions to engineer section with deadlines.

8-5. Base Camp Design Data — ATP 3-37.10

Base camp design data in MSS integrates survivability planning with the broader base camp layout. IAW ATP 3-37.10, base camp design must account for force protection requirements from initial planning.

Base Camp Data Elements in MSS: - Base camp designation, grid center, and perimeter trace - Planning population (personnel and vehicles) - Layout by zone: life support area, vehicle and equipment area, headquarters area, ammunition holding area, medical area - Force protection features: standoff distances from perimeter wire, ECP locations, internal barriers, blast walls - Engineer resources: HESCO quantities, concertina wire linear footage, sandbag quantities - Utilities: electrical, water, fuel point locations - Aviation landing areas (if applicable) - Status: Planned, Under construction, Operational, Closing

CHAPTER 9 — ECHELON-SPECIFIC PROTECTION OPERATIONS

BLUF: Protection tasks and MSS data responsibilities shift by echelon. Company-level focuses on local execution; battalion integrates data across subordinate companies; BCT coordinates the protection working group and synchronizes all protection functions; division and corps manage theater-wide protection data and AT program oversight.

9-1. Company/Battery Level

At company and battery level, protection data management is focused on execution and local reporting. The company XO or first sergeant is the senior protection data manager at this echelon. Dedicated protection staff positions (CBRN officer, AT officer, PMO) are generally not organic at company level — protection tasks are additional duties.

Company-Level MSS Protection Tasks: - Enter CRM risk assessments for all training and operations events (Chapter 2) - Report CBRN detection events to battalion CBRN officer via MSS event entry (Chapter 3) - Maintain ECP status for company patrol bases or observation posts (Chapter 5) - Update fighting position status in survivability layer (Chapter 8) - Enter AT-relevant incidents for aggregate reporting to battalion AT officer

Company-Level Protection Data Standard: - At minimum: CRM data for all events, CBRN event reports within 15 minutes, ECP status at shift change

9-2. Battalion Level

The battalion S2 and the battalion AT officer (additional duty in most battalions) coordinate protection data across the battalion. The S6 manages MSS connectivity for the protection workspace. The CBRN officer (if assigned as a specialty officer) manages the CBRN data layer.

Battalion MSS Protection Integration Points: - S2/S3 integration: threat data from S2 feeds AT officer FPCON assessment - CBRN/S4 integration: decontamination resupply requirements visible in logistics workspace - PMO/S3 integration: SIR data linked to operations reporting chain - Engineer/S3 integration: survivability position data briefed at planning meetings

Key Battalion Protection PWG Data Products: - Combined CBRN threat overlay (aggregated from company reports) - FPCON status and RAM execution rate - AT incident log with status - Survivability position completion status (percent of planned positions constructed) - Detection equipment FMC rate across battalion

9-3. Brigade Combat Team (BCT) Level

The BCT has a designated protection officer (typically a functional area 50 series or branch-qualified field grade officer on the brigade staff). The protection officer chairs the Protection Working Group, which meets IAW the brigade battle rhythm.

BCT Protection Officer MSS Responsibilities: - Maintain the brigade-level protection workspace - Synchronize protection data contributions from all subordinate battalions and attached elements (CBRN company, MP platoon, ADA battery, engineer battalion) - Produce the brigade protection assessment product for the commanding general (or brigade commander's) weekly review - Coordinate AT program data with the brigade AT officer - Manage the CAL/DAL with the brigade AMD officer (14A) - Brief protection status at the PWG and the brigade weekly update

BCT Protection Working Group — MSS Data Agenda: 1. CBRN threat update (CBRN officer) 2. FPCON status and RAM execution (AT officer) 3. ECP status and physical security summary (PMO) 4. AMD air picture and ADW status (ADA officer) 5. Survivability status (engineer) 6. CRM residual risk summary (safety officer) 7. Open AT incidents and SIRs (AT officer / PMO) 8. Action items from previous PWG — status

9-4. Division and Corps

At division and corps, the protection officer is a senior field grade officer, and the protection cell includes dedicated CBRN, AT, AMD, engineer, and legal staff. MSS at division and corps provides theater-wide protection data visibility and supports the theater AT program.

Division/Corps Protection MSS Functions: - Theater CBRN threat overlay (aggregated from subordinate formations plus theater CBRN intelligence) - Theater FPCON management (USAREUR-AF level FPCON direction) - Theater AT program management: annual AT review data, installation AT officer coordination, theater vulnerability assessment cycle - Theater AMD management: THAAD/Patriot data, AAMDC coordination, theater CAL/DAL - CBRN defense planning data for theater CBRN response force - Legal coordination (27A): law of armed conflict (LOAC) data inputs to AT ROE, legal review of C-UAS engagement rules

9-4a. Legal Support to Protection — 27A Role in MSS

The unit judge advocate (27A) provides legal support to protection operations through several MSS-integrated functions. While legal advisory work occurs through standard SJA channels, the 27A should be integrated into the protection workspace for AT and C-UAS data coordination.

27A MSS Functions in Protection:

AT Legal Review: The SJA reviews AT vulnerability assessments to ensure recommended countermeasures comply with SOFA provisions, local laws, and command authority. Specific countermeasures that affect local national personnel, contractors, or civilian vehicles at ECPs require legal review. The AT officer links the legal review note to the assessment record in MSS.

ROE Coordination: C-UAS engagement rules, ECP ROE, and the use of force in physical security contexts are documented with SJA coordination. The SJA provides a legal review annotation in MSS for standing ROE documents linked to the AT workspace. This is not the ROE document itself — it is a record that legal review occurred and the reference to the current ROE card.

C-UAS Engagement Review: After any C-UAS defeat action, the SJA reviews the engagement record for legal compliance. The 27A enters a "Legal Review Complete" annotation in the MSS C-UAS event record with a brief assessment (Compliant, Requires Further Review, Referred for Investigation). This annotation is not a public legal opinion — it is a command record indicating legal review was conducted.

Detainee and Resettlement Coordination: In environments where the unit conducts internment operations, the 27A coordinates MSS tracking data for detainees with the PMO. Legal review of detention status is annotated in the relevant records per the Law of Armed Conflict and applicable command directives.

NOTE: MSS data related to legal proceedings, investigations, or detainee status may be subject to special handling requirements under legal privilege and AR 27-series regulations. Coordinate with the SJA before sharing or exporting any data in these categories outside the originating workspace.

Table 9-1. Protection Data Ownership by Echelon

Data Domain	Company	Battalion	BCT	Div/Corps
CRM Data	Enters	Aggregates/Reviews	Program oversight	Theater trend analysis
CBRN Threat	Reports	Maintains overlay	Synchronizes	Theater-wide threat picture
FPCON	Executes measures	Updates, reports	Manages for formation	Directs theater FPCON
AT Assessment	Not primary	Conducts (addl duty)	AT officer manages	Theater AT program
ECP/Physical Security	Manages local	Reviews battalion	PMO coordinates	Installation security oversight
AMD/CAL-DAL	Receives ADW	S2 coordinates	ADA battery manages	AAMDC/theater AMD
Survivability	Constructs, reports	Monitors, priorities	Engineer plan	Not primary

CHAPTER 10 — DEGRADED OPERATIONS

BLUF: Protection operations continue when MSS is degraded. Manual procedures, PACE plans, and minimum essential products ensure the unit maintains protection capability across all six functions regardless of MSS availability. The protection data accumulated in MSS is only valuable if backup systems exist when the platform is unavailable.

10-0. Degraded Operations Mindset

The standard for protection data management is not MSS availability — it is continuous protection coverage. MSS enables faster, more integrated protection data management. But no protection function should be wholly dependent on MSS availability. Leaders who have designed their protection program around the assumption that MSS will always be available have created a single point of failure.

The degraded operations procedures in this chapter are not emergency measures — they are the baseline protection capability the unit maintains regardless of MSS status. Units that practice manual fallback procedures regularly will execute them confidently when MSS is unavailable. Units that do not practice will fail at a critical moment.

NOTE: Include degraded operations drills in unit MSS training. At least once per quarter, the protection officer should direct a 30-minute "no MSS" drill in which the protection cell maintains all required protection data using manual methods. The drill reveals which protection tasks are genuinely executable without MSS and which have been over-dependent on the platform.

10-1. Protection Operations When MSS Is Degraded

MSS degradation scenarios for protection practitioners: - Network outage at unit level (local connectivity lost, MSS accessible at higher echelon) - Server or platform outage (MSS unavailable formation-wide) - Power failure at CP (MSS displays offline until generator restored) - Cybersecurity incident (MSS taken offline by C2DAO direction) - Communications degradation preventing data push to/from MSS

In all degradation scenarios, protection tasks continue. Data accumulates in manual formats and is entered retroactively when MSS is restored.

10-2. Manual AT Reporting Backup

The AT officer maintains a printed AT backup package at all times. This package is the AT officer's fallback when MSS is unavailable.

AT Backup Package Contents: - Current threat assessment summary (printed, dated within 30 days) - Current FPCON level and measures (printed, signed by commander) - RAM schedule for current cycle (printed, not electronic) - AT incident log (blank forms for manual entry during outage) - FPCON change authority matrix (who can change FPCON at this echelon) - Emergency contact directory for AT reporting chain

10-3. CBRN Backup Procedures

CBRN reporting does not stop because MSS is unavailable. IAW FM 3-11, CBRN reports use established voice and digital reporting channels.

CBRN Fallback Reporting: - NBC 1–6 reports transmit via voice on the NBC reporting net (see unit CEOI) - Paper NBC report forms are maintained in the CBRN kit - Contamination overlays revert to acetate map overlay (1:50,000 scale minimum) - Detection equipment status is tracked on a printed equipment roster - Decontamination site locations are maintained on the acetate overlay

When MSS is restored, the CBRN officer enters all events, reports, and status changes from the outage period as retroactive entries with the original event DTGs — not the entry DTG.

NOTE: Retroactive MSS data entry after an outage must use the actual event DTG, not the time of entry. Entering all outage-period data with the restoration timestamp destroys the temporal accuracy of the CBRN data record and makes post-event analysis unreliable.

10-4. PACE Plan for Protection Data

The Protection WFF PACE plan defines the data management methods for each contingency:

Table 10-1. Protection Data PACE Plan

System	Primary	Alternate	Contingency	Emergency
AT reporting	MSS protection workspace	SIPRNET email to battalion S3	VINSON/SINCGARS on AT reporting net	Physically report to battalion TOC
CBRN reporting	MSS CBRN workspace	Digital NBC report via SIPRNET	Voice NBC report on NBC reporting net	Messenger to battalion CBRN officer
FPCON notification	MSS alert notification	SIPRNET message to subordinate commanders	Voice on command net	Mounted courier
Physical security status	MSS ECP layer	MP duty log (paper)	CP/TOC whiteboard	Voice report at guard change
CRM tracking	MSS CRM workspace	Local file (encrypted)	Paper DA Form 7566	Command decision without documentation

10-5. Minimum Essential Protection Products Without MSS

When MSS is fully unavailable, the protection officer maintains these minimum essential products:

1. **Protection overlay** — acetate on current operations map; CBRN hazard areas, ECP locations, AMD positions, survivability positions in standard military symbols
2. **FPCON board** — physical display at CP showing current FPCON and required measures
3. **AT incident log** — paper log, chronological

4. **CBRN status card** — hand-written, shows: current threat, detection status, CCP locations, decon site status
5. **Protection working group minutes** — hand-written agenda and action items from each PWG meeting

10-5a. Protection Data — Before/During/After Operations Checklist

The following checklist organizes the protection officer's MSS data actions across the operational cycle. Use this checklist during MDMP, during execution, and during assessment.

BEFORE Operations (Planning and Preparation Phase):

Action	Responsible	Standard
Verify CBRN threat overlay is current	CBRN Officer	Data-as-of within 24 hours; source cited
Verify AT vulnerability assessments for all facilities on the route/in the AO	AT Officer	Within 180 days; threat data current
Confirm current FPCON in MSS matches command-directed FPCON	AT Officer	Verified against issuing authority within 24 hours
Load CRM risk assessments for all mission tasks	All section leaders	Approved by required authority before execution
Verify CAL/DAL is current for the AO	ADA Officer	Reviewed within 30 days; DAL reflects current AMD asset disposition
Confirm survivability data is current for all positions used	Engineer Section	Updated within 72 hours
Brief MSS degraded operations PACE plan with subordinates	Protection Officer	Confirmed understood by all protection WFF contributors
Conduct workspace sharing check	Protection Officer	CBRN, AT, AMD, Physical Security layers accessible to S3 and subordinates

DURING Operations (Execution Phase):

Action	Trigger	Standard
Enter CBRN detection event	On initial detection	Within 10 minutes; NBC 1 data entered
Issue NBC 3 warning	On decision to warn	Within 10 minutes of decision; geospatial overlay plotted
Update FPCON	On command direction	Within 15 minutes of direction; all subordinate workspaces notified

Action	Trigger	Standard
Enter AT incident	On incident occurrence	Within 1 hour of incident
Update ECP status	On any status change	Within 30 minutes of change; at every shift change
Enter C-UAS detection	On UAS detection	Within 5 minutes of first detection
Update survivability position status	On completion or damage	Within 24 hours of status change

AFTER Operations (Assessment Phase):

Action	Timeframe	Standard
Close open CBRN events with final status	Within 24 hours of event conclusion	Agent confirmed or marked unknown; hazard area marked cleared or still active
Update AT incident records with resolution	Within 72 hours	Lessons learned entered; corrective actions assigned
Update CRM records with control verification data	Within 24 hours of task completion	Each control marked verified or not verified with note
Conduct PWG after any significant protection event	Within 48 hours	Data from event reviewed; corrective actions assigned in MSS
Submit C-UAS post-event report	Within 2 hours of event conclusion	All defeat actions documented; engagement authority recorded
Update survivability deficiency status	Within 7 days of assessment	Corrective actions marked in progress or complete

10-6. Reconstitution After Outage

When MSS is restored: 1. The CBRN officer enters all retroactive CBRN event and report data first — CBRN data has the highest operational risk from gaps. 2. The AT officer updates FPCON data and any AT incidents that occurred during the outage. 3. The PMO desk officer enters incident log entries from the outage period. 4. The survivability NCO updates any position status changes. 5. The CRM workspace is updated with any risk assessments completed on paper during the outage. 6. The protection officer verifies the integrated protection picture is current and accurate before the next PWG or briefing cycle.

APPENDIX A — PROTECTION NAMING CONVENTIONS IN MSS

Consistent naming is essential for searchability, cross-unit data sharing, and automated alert functions. All protection data entries in MSS follow these naming conventions.

A-1. General Convention Format: `[UNIT]-[TYPE]-[IDENTIFIER]-[YYYYMMDD]`

Examples: - `1-16IN-CBRN-EVENT-20260312` — CBRN event entry, 1-16 Infantry, 12 March 2026 - `2BCT-AT-ASSESS-FOB_WIESB-20260301` — AT vulnerability assessment, 2BCT, FOB Wiesbaden, 1 March 2026 - `PMO-ECP-01-STATUS-20260312` — ECP 1 status entry, 12 March 2026 - `2BCT-SURV-FP-BP27-20260310` — Survivability fighting position, Battle Position 27

A-2. CBRN Data Naming: - Contamination overlays: `[UNIT]-CBRN-OVERLAY-[AGENT]-[YYYYMMDDHHMMZ]` - NBC reports: `[UNIT]-NBC[1-6]-[YYYYMMDDHHMMZ]` - CCP entries: `[UNIT]-CCP-[NUMBER]-[YYYYMMDD]`

A-3. AT Data Naming: - FPCON entries: `[UNIT]-FPCON-[LEVEL]-[YYYYMMDDHHMMZ]` - RAM entries: `[UNIT]-RAM-[MEASURE_CODE]-[YYYYMMDD]` - AT incidents: `[UNIT]-AT-INC-[SEQUENTIAL_NUMBER]-[YYYYMMDD]`

A-4. Physical Security Naming: - ECP entries: `[UNIT]-ECP-[NUMBER]-[YYYYMMDD]` - SIR entries: `[UNIT]-SIR-[SEQUENTIAL_NUMBER]-[YYYYMMDD]`

APPENDIX B — CBRN REPORT FORMATS: NBC 1–6 QUICK REFERENCE

B-1. NBC 1 Report — Initial CBRN Observation Initial report from observer. Transmitted immediately. Format: - Line 1: Report type (NBC 1) - Line 2: Observer's callsign - Line 3: Location of attack/event (grid) - Line 4: Date-time of attack/event (DTG, Zulu) - Line 5: Type of attack: Nuclear/Biological/Chemical/Radiological - Line 6: Method of delivery (if observed): aircraft, missile, artillery, ground release, unknown - Line 7: Direction of attack (if from a vector)

B-2. NBC 2 Report — Evaluated Data Staff-evaluated compilation. Format: - Lines as NBC 1 plus: - Line 8: Detailed description of attack - Line 9: Confirmation of agent type (if assessed)

B-3. NBC 3 Report — Immediate Warning Warning of CBRN danger to other units. Format: - Agent type - Hazard area (grid-defined) - Time hazard valid from/to - Recommended protective actions

B-4. NBC 4 Report — Monitoring and Survey Results Results of reconnaissance. Format: - Monitoring equipment used - Readings (dose rate or concentration, by location) - Grid of each reading - DTG of each reading - Agent identified (if conclusive)

B-5. NBC 5 Report — Completed Hazard Prediction Formal hazard overlay. Format: - Prediction model and version - Input parameters (met data: wind, stability, temperature) - Hazard zone boundary data (series of grid coordinates) - Validity period

B-6. NBC 6 Report — Detailed Technical Data Post-laboratory or technical analysis. Format: - Sample type and collection DTG - Analyzing agency - Agent confirmed (specific agent identification) - Concentration or dose data - Confidence level: Confirmed, Probable

APPENDIX C — FPCON MEASURES REFERENCE

Table C-1. FPCON Measures by Level (Selected — IAW DOD O-2000.12-H)

Measure	NORMAL	ALPHA	BRAVO	CHARLIE	DELTA
AT awareness training	Annual	Current	Current	Current	Current
Random security checks	No	Yes	Yes	Increased	Maximum
Vehicle inspection at ECPs	Visual	Visual	100% exterior	100% exterior + interior	Full sweep
Access roster verification	SOF	SOF	All visitors	All personnel	All personnel + escort
Mail/package inspection	No	No	100%	100%	100% + X-ray
Suspicious activity reporting	Standard	Heightened	Heightened	Maximum	Maximum
QRF availability	On call	On call	On alert	Standby	Deployed
CBRN equipment status	Ready	Ready	100% FMC	100% FMC	100% FMC + staged

Note: This table is representative, not exhaustive. Refer to the current USAREUR-AF FPCON measures directive for the complete measures list.

APPENDIX D — PROTECTION WORKING GROUP CHECKLIST

D-1. Pre-PWG Data Preparation (NLT 2 hours before PWG) - ☐ CBRN officer: Update contamination overlay, verify data-as-of timestamp is current - ☐ AT officer: Verify FPCON is current in MSS; pull RAM execution rate for the period - ☐ PMO: Pull incident/SIR log for the period; verify ECP status is current - ☐ AMD officer: Verify ADW status is current; pull CAL/DAL update if changes pending - ☐ Engineer: Pull survivability position completion status - ☐ Safety officer: Pull CRM data — any open High-risk assessments or pending approvals - ☐ Protection officer: Review all data before the PWG; identify gaps or anomalies

D-2. PWG Meeting — Standard Agenda 1. Current threat assessment (S2 representative) — 5 min 2. CBRN update (CBRN officer) — 5 min 3. FPCON status and RAM execution (AT officer) — 10 min 4. Physical security and incident status (PMO) — 10 min 5. AMD/ADW status (ADA officer) — 5 min 6. Survivability status (engineer) — 5 min 7. CRM open items (safety officer) — 5 min 8. Action items from previous PWG — 5 min 9. New action items — as required

D-3. Post-PWG Actions (NLT 24 hours after PWG) - ☐ Protection officer: Enter PWG minutes in MSS protection workspace - ☐ All action item owners: Enter new action items in MSS with due date and responsible party - ☐ AT officer: Update any FPCON or RAM changes directed at PWG - ☐ CBRN officer: Update any CBRN data actions from PWG

APPENDIX E — AT RISK ASSESSMENT DATA FIELDS

E-1. Mandatory Data Fields for All AT Assessments in MSS

Field	Description	Required?
Assessment ID	Auto-generated on creation	Yes
Facility/Location name	Common name of assessed location	Yes
Facility type	FOB, COP, transit site, key facility, etc.	Yes
Grid location	8-digit MGRS	Yes
Assessment date	Date assessment conducted	Yes
Next review date	Auto-calculated (180 days default)	Yes
Threat source	Group or general threat category	Yes
Threat categories assessed	Select all that apply	Yes

Field	Description	Required?
CARVER + Shock scores	All 7 categories, 1–10 scale	Yes
Overall vulnerability score	Calculated from CARVER + Shock	Auto
Threat probability	H/M/L with rationale	Yes
Overall AT risk	Calculated: Threat × Vulnerability	Auto
Existing countermeasures	List with implementation status	Yes
Recommended countermeasures	Prioritized list	Yes
Approving authority name	Name and position	Yes
Approving authority signature	Electronic signature in MSS	Yes
Classification	UNCLASSIFIED, CUI, or higher	Yes

APPENDIX F — MOS DUTY POSITION CROSS-REFERENCE QUICK CARD

F-1. Purpose. This card provides a rapid reference for each MOS covered by SL 4E. Use this card to identify which chapters apply to your duty position and what your primary MSS data responsibilities are.

Table F-1. MOS Quick Reference

MOS	Title	Primary Duty Position(s)	Key MSS Data Responsibilities	Priority Chapters
74A	CBRN Officer	Chemical Officer, CBRN Officer, NBC Staff Officer	CBRN workspace management, NBC report entry, contamination overlay currency, detection equipment tracking, decon site management	1, 2, 3, 8, 9, 10
74D	CBRN Specialist	CBRN NCO, CBRN Recon Specialist, Decon NCO	NBC report data entry, detection equipment status updates, CCP status entry, field overlay reporting	3, 8, 9
31A	Military Police Officer	Provost Marshal Officer, PMO, MP Platoon Leader	Physical security workspace management, ECP data management, SIR entry and approval, incident trend review, PWG physical security brief	1, 4, 5, 9, 10

MOS	Title	Primary Duty Position(s)	Key MSS Data Responsibilities	Priority Chapters
31B	Military Police	MP, Patrol Officer, Gate Guard, Desk Officer	ECP status entry at shift change, incident report entry, SIR initial entry for desk officer review	5, 9
31D	Criminal Investigation Agent	CID Special Agent	AT incident data (investigative referrals), SIR coordination with PMO, forensic/evidence tracking (separate from MSS — MSS is the AT record only)	4, 5
14A	ADA Officer	ADA Battery Commander, AMD Officer, SHORAD Officer	AMD workspace management, CAL/DAL management, ADW tracking and notification, AMD engagement record entry, airspace deconfliction data	1, 6, 9
14E	Patriot Fire Control Operator	Patriot FCS Operator/Maintainer	AMD system status entry, engagement record entry, battery operational status updates	6
14P	Air Defense EWS Operator	AEWS Operator, Air Defense Warning System	ADW status updates, air track manual entry when required, early warning data entry	6
14S	AMD Crewmember	AMD Crew (SHORAD/Avenger/Stinger)	Local air track reporting, AMD system employment status, C-UAS detection entry at team level	6, 9
12B	Combat Engineer	Combat Engineer, Sapper, Engineer Platoon Leader	Survivability position entry, fighting position status updates, obstacle data, base camp design data layer	8, 9
12R	Interior Electrician	Base Camp Electrician, Facilities Engineer	Facility hardening status (electrical infrastructure), base camp utilities data, generator and electrical site status	8
27A	Judge Advocate	SJA, Legal Advisor, Brigade JA	Legal review documentation linked to AT incidents, ROE reference data, C-UAS engagement authority data, LOAC coordination	4, 5
37F	PSYOP Specialist	MISO Team Member, PSYOP NCO, IO Cell	MISO and OPSEC coordination data linked to AT workspace, threat messaging tracking, MISO product linkage to AT picture	4
180A	SF Warrant	Special Forces Senior Warrant, Team	Base defense planning data, AT assessment (SOF-specific), survivability for unconventional	4, 5, 8

MOS	Title	Primary Duty Position(s)	Key MSS Data Responsibilities	Priority Chapters
	Officer	Sergeant	environments	
311A	CI Warrant Officer	CI Warrant, COUNTERINT Officer	AT intelligence data (CI portion), insider threat indicator tracking, AT-CI coordination in MSS workspace	4
311B	CI Special Agent	CI Agent, HUMINT Collector (CI)	AT incident data (CI-relevant), insider threat report entry, liaison with AT officer data	4

F-1a. Cross-Reference to Related TMs

Related TM	Relevance to Protection WFF
SL 1 (Maven User)	Foundation prerequisite. Platform navigation, basic data access. Required before this manual.
SL 2 (Builder)	Required as prerequisite (Go evaluation on file). Builder skills are not exercised in this track — SL 4E practitioners consume pre-built products. The SL 2 cert is part of the progression chain to SL 3.
SL 3 (Advanced Builder)	Required prerequisite (Go evaluation on file). Advanced builder skills are not exercised in this track. SL 3 completion certifies platform literacy at the level required before WFF track enrollment.
SL 4A (Intelligence)	AT intelligence integration; threat data for AT assessments
SL 4B (Fires)	AMD coordination — fires and protection share AMD data domain
SL 4C (Movement and Maneuver)	Physical security integration with maneuver operations; base camp siting
SL 4D (Sustainment)	CBRN resupply coordination; medical tracking for CBRN casualties
SL 4F (Mission Command)	COP integration; CCIR and decision support products that consume protection data
SL 4G–O (Specialist Tracks)	Post-graduate technical tracks (prereq SL 3). Not required for protection WFF employment.
SL 5G–O (Advanced Specialist Tracks)	Advanced technical tracks (prereq SL 4G–O). Not applicable to operational protection practitioners.

F-2. New User Checklist. Before using the MSS protection workspace for the first time, verify:

- ☐ SL 1 complete — can log in, navigate Workshop, access assigned datasets
- ☐ CONCEPTS_GUIDE_TM40E complete — protection WFF / MSS integration understood

- ☐ MSS account provisioned with correct role for your workspace zone — coordinate with unit S6
- ☐ Workspace zones identified — know which workspace zone corresponds to your MOS function
- ☐ Naming convention reviewed — Appendix A; use correct format for all entries
- ☐ Classification guidance briefed by unit IMO — know the classification level for your data type
- ☐ PWG meeting schedule confirmed — know when Protection Working Group meets and what data you must prepare

---

APPENDIX G — PROTECTION WORKING GROUP DATA STANDARDS

G-1. Purpose. This appendix defines the minimum data quality standards for each protection workspace zone. These standards apply at the BCT level and above. Lower echelons should scale standards to available resources.

G-2. CBRN Zone Standards

Data Element	Standard	Review Frequency
Contamination overlay	Data-as-of within 6 hours; meteorological data source cited; confidence level marked on each hazard area	Before every PWG and before every commander's brief
NBC reports	All received NBC reports entered within 15 minutes of receipt; all 6 report types formatted correctly; source and confidence level recorded	Continuous during CBRN events
CCP status	Active CCPs updated minimum every 4 hours; closed CCPs marked closed with DTG within 1 hour of closure	Continuous when CCP is active
Detection equipment	FMC/PMC/NMC status current; NMC equipment has estimated return-to-FMC date; last calibration date current	Weekly minimum; before all operations
Decon site status	Operational/standby/closed status current; throughput capacity and water source entered	Before all operations with CBRN threat

G-3. AT Officer Zone Standards

Data Element	Standard	Review Frequency
FPCON level	Current command-directed FPCON entered with authority citation and effective DTG within 15 minutes of direction	Continuous; any FPCON change
AT assessment	All active assessments reviewed within 180 days; countermeasure status current; threat data sourced within 90	Semi-annual minimum; after any threat change

Data Element	Standard	Review Frequency
s	days	
RAM schedule	Current RAM schedule entered; execution status marked within 24 hours of each RAM window	Weekly execution status review
AT incidents	All incidents entered within 1 hour; open incidents have status update within 72 hours; closed incidents have lessons learned	Continuous

G-4. PMO Zone Standards

Data Element	Standard	Review Frequency
ECP status	All active ECPs updated at each shift change (minimum every 8 hours)	Every shift change
Perimeter trace	Accurate to within 100 meters; updated within 24 hours of any physical change	After any perimeter change
Incidents/SIRs	Entered within 1 hour of reportable incident; SIR submitted within 2 hours of determination; all open SIRs have status	Continuous

G-5. AMD Zone Standards

Data Element	Standard	Review Frequency
ADW status	Current ADW entered with source citation and effective DTG within 10 minutes of direction	Continuous; any ADW change
CAL/DAL	All CAL assets entered with DAL designation; accepted risk documented for non-DAL CAL assets	Monthly minimum; after mission change
AMD system status	FMC/PMC/NMC status current for all AMD systems; location current	Daily

G-6. Survivability Zone Standards

Data Element	Standard	Review Frequency
Fighting positions	All planned positions entered; status (planned/under construction/complete) current within 24 hours	Daily during construction
Facility hardening	All priority facilities assessed; hardening level current; deficiencies with corrective action assigned	Weekly
CCD plan	CCD measures entered for all priority positions; last inspection date current	Weekly

APPENDIX H — PROTECTION OFFICER'S WEEKLY MSS REVIEW CHECKLIST

Purpose. The protection officer conducts a weekly MSS review independent of the PWG to verify data quality across all zones. This checklist guides that review.

H-1. Weekly Review Procedure

Complete the following in order. Note any data quality issue and assign correction action with due date.

CBRN Zone Review: - ☐ Contamination overlay: data-as-of timestamp. Is it within required standard? _ - ☐ Any open CBRN events not closed or updated? _ - ☐ Detection equipment: any NMC equipment without a return-to-FMC estimate? _ - ☐ Any NBC reports received this week not entered in MSS? _

AT Officer Zone Review: - ☐ FPCON: matches current command direction? Verified against authoritative source? _ - ☐ Any AT assessments past 180-day review date? _ - ☐ RAM execution rate this week: _% (below 85% requires command attention) - ☐ Any open AT incidents older than 72 hours without a status update? _

PMO Zone Review: - ☐ Any ECPs with status older than 8 hours (missed shift-change update)? _ - ☐ Any open SIRs without 72-hour status update? _ - ☐ Perimeter trace accurate (no physical changes without MSS update)? _

AMD Zone Review: - ☐ ADW status: matches current AAMDC/theater AMD direction? _ - ☐ CAL/DAL reviewed within 30 days? Last review date: _ - ☐ Any AMD systems NMC without estimated return-to-FMC? _

Survivability Zone Review: - ☐ Any planned positions not updated to "complete" when physically complete? _ - ☐ Facility hardening status: any priority facilities without a current assessment? _

Cross-Zone: - ☐ Any workspace sharing gaps — data that exists but is not visible to S2/S3/subordinate units? _ - ☐ Any classification level concerns identified this week? _ - ☐ Next PWG data ready (CBRN, AT, PMO, AMD, Survivability briefs prepared)? _

APPENDIX I — 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	"Exploring AI-Enhanced Cyber and Information Ops Integration"	Mar-Apr 2025	AI in cyber defense

Source	Title	Date	Relevance
Army Communicator	"Leading in Data Centricity, C2 Fix Best Practices"	Spring 2025	Data-centric protection operations
Military Review	"Advancing Counter-UAS Mission Command Systems"	May-Jun 2024	C-UAS and data integration

GLOSSARY

Air Defense Warning (ADW): A DOD-standardized system for communicating air threat levels. Levels are WHITE (no attack imminent), YELLOW (attack probable), and RED (attack imminent or occurring). ADW status is tracked in the MSS AMD workspace.

Antiterrorism (AT): Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts, to include limited response and containment by local military and civilian forces (JP 3-07.2). AT data in MSS includes vulnerability assessments, FPCON tracking, and RAM management.

CARVER + Shock: An assessment methodology for evaluating the vulnerability of a target or asset to attack. Factors: Criticality, Accessibility, Recuperability, Vulnerability, Effect, Recognizability, and Shock (social, economic, or psychological impact). Used in AT vulnerability assessments.

Contamination Control Point (CCP): A location established to perform decontamination on personnel and/or equipment during or following CBRN operations. CCP locations, type, and status are tracked in the MSS CBRN workspace.

Counter-UAS (C-UAS): Actions taken to detect, identify, track, and defeat hostile unmanned aircraft systems. C-UAS data tracked in MSS includes detection events, identification assessments, and defeat actions.

Critical Asset List (CAL): A prioritized list of assets or areas, normally identified by a commander, that must be protected from loss, damage, or exploitation (JP 3-01). The CAL in MSS links to the DAL to show AMD coverage gaps.

Defended Asset List (DAL): The subset of CAL assets that an AMD force can defend given available resources. The difference between the CAL and DAL represents accepted risk, which must be documented in MSS.

Force Protection Condition (FPCON): DOD's principal means of terrorism threat communication and standardizing protective measures. Five levels: NORMAL, ALPHA, BRAVO, CHARLIE, DELTA. FPCON is tracked in the MSS AT officer zone with full change log.

Hazard Prediction: A calculation or model-based estimate of the area expected to be affected by a CBRN hazard under given meteorological conditions. Hazard predictions are entered in the MSS CBRN workspace as geospatial overlay data with a validity period.

NBC Report: Standard military report formats for nuclear, biological, or chemical events. Six types (NBC 1–6), each covering a phase of the CBRN event cycle from initial observation through technical analysis. All six types are entered in the MSS CBRN workspace.

Protection Working Group (PWG): A recurring meeting that synchronizes protection tasks across WFFs and functional cells. The PWG is the primary venue for protection data review and synchronization on MSS.

Random Antiterrorism Measures (RAM): Security measures implemented on an unpredictable schedule to deny threat actors the ability to identify patterns in unit security posture. RAM is managed in the MSS AT officer zone with a scheduling and execution tracking function.

Serious Incident Report (SIR): A report of any incident involving death, serious injury, substantial property damage, or other significant event that requires command attention IAW AR 190-40. SIRs are entered in the MSS PMO zone and submitted up the reporting chain.

Survivability Operations: Actions that protect friendly forces, supplies, equipment, and facilities from the effects of enemy weapons and hazards (ATP 3-37.34). Survivability data tracked in MSS includes fighting positions, facility hardening status, and CCD plan data.

SL 4E — Maven Smart System: Protection Warfighting Function Headquarters, United States Army Europe and Africa Wiesbaden, Germany — 2026

Next scheduled review: March 2027 Submit corrections or recommendations to: USAREUR-AF C2DAO, Wiesbaden, Germany

DoD and Army Strategic References:

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