Standard Operating Procedure

Expert-Driven AI-Assisted Development

A Methodology for Building Institutional Capability

Document Version: 3.0
Effective Date: 26 January 2026
Classification: UNCLASSIFIED // Distribution Unlimited

Prepared by:
SSgt Jesse C. Morgan
Marine Corps Detachment, Presidio of Monterey
Defense Language Institute Foreign Language Center

Core Principle:

Use AI to build things that don't need AI.

The tools last. The AI was just how we built them.

Contents

1. Purpose and Scope

1.1 Purpose

This Standard Operating Procedure establishes the methodology for subject matter experts to develop permanent institutional tools using AI-assisted development.

This SOP is NOT about:

- Making personnel dependent on AI
- Using AI to perform daily tasks
- Replacing human judgment with automation

This SOP IS about:

- Empowering experts to build permanent solutions
- Creating institutional capability that outlives individuals
- Using AI as scaffolding to construct lasting tools

1.2 Scope

This methodology applies to any military or civilian personnel who:

- Possess domain expertise in a problem area
- Seek to build a solution rather than wait for one
- Are willing to complete required training and follow this SOP

No programming background is required. Domain expertise is the prerequisite.

1.3 Applicability

This SOP is designed for adaptation by any DoD unit. While developed at Marine Corps Detachment, Presidio of Monterey, the methodology applies to training commands, operational units, and support organizations—any environment where experts have problems to solve.

2. The Four-Layer Framework

2.1 Layer 1: Direct Tool Development

Experts build applications that solve their own problems. The person who understands the problem builds the solution—no middlemen, no requirements documents, no months of waiting.

2.2 Layer 2: Process Liberation

Automate routine work to surface insights for human judgment. Dashboards inform intuition; they don't replace it.

2.3 Layer 3: Capability Cultivation

Develop personnel who want to become builders. One builder per section creates capability for the entire section.

2.4 Layer 4: Documentation and Replication

Design all tools for rebuild, not merely maintenance. Tools must survive PCS cycles to become institutional capability.

3. The Creator Mindset

3.1 Consumer vs. Creator

AI Consumer (Avoid)	AI-Enabled Creator (Goal)
"Help me do this task"	"I'll build a tool that solves this permanently"
Temporary assistance	Permanent artifact
No lasting output	Tool serves the unit
Dependence grows	Capability grows
Individual benefit	Institutional benefit

3.2 The Artifact Test

After any AI interaction, ask:

> *Does a permanent artifact exist that delivers value without further AI involvement?*

- **If YES:** You are creating institutional capability.
- **If NO:** You are consuming AI assistance.

4. Compliance and Security Requirements

Compliance Note: The requirements in this section exist to protect you, your unit, and the people whose data you handle. Most tools built under this SOP won't trigger additional reviews—but knowing the rules upfront saves headaches later.

4.1 Data Classification

4.1.1 Prohibited in AI Prompts

The following shall not be entered into AI tools:

- Classified information (any level)
- Controlled Unclassified Information (CUI) unless AI tool is authorized for CUI
- Personally Identifiable Information (PII) unless explicitly authorized

- Protected Health Information (PHI)
- Operational plans, schedules, or intelligence products
- For Official Use Only (FOUO) information

4.1.2 Personally Identifiable Information (PII)

PII includes: Social Security Numbers, dates of birth, home addresses, personal phone numbers, financial information, medical information, biometric data, or any combination that could identify an individual.

Before including ANY PII in a tool:

1. Obtain written approval from the Privacy Officer
2. Complete Privacy Impact Assessment (if required)
3. Implement required safeguards
4. Document data handling procedures

4.1.3 Protected Health Information (PHI)

PHI is governed by HIPAA and DoD health information policies. Tools handling PHI require coordination with medical/health information management, legal review, specific security controls, and Business Associate Agreement if applicable.

Simple rule: Unless your command specifically directs you to build a tool handling health data, don't. If they do, they'll provide the oversight.

4.2 Privacy Requirements

4.2.1 Privacy Impact Assessment (PIA)

A PIA may be required when a tool:

- Collects PII from 10 or more individuals
- Creates a new system of records
- Significantly modifies an existing system containing PII
- Uses PII in a manner not previously authorized

Process: Complete PIA Threshold Analysis (Appendix D). If threshold met, coordinate with unit Privacy Officer before proceeding.

4.2.2 System of Records Notice (SORN)

If a tool creates records retrievable by individual identifier, a SORN may be required under the Privacy Act. Coordinate with Privacy Officer and legal staff.

4.2.3 Appeals Process

If the Privacy Officer or Cybersecurity Office denies a tool request:

1. Request written explanation of specific concerns
2. Work with office to identify acceptable modifications
3. If modifications satisfy concerns, resubmit with changes documented
4. If impasse remains, escalate through chain of command with documentation of business need and proposed mitigations

Most denials result from misunderstanding the tool's scope. Clarifying conversations often resolve issues without formal appeal.

4.3 Cybersecurity Requirements

4.3.1 Approved AI Tools

Only use AI tools approved for government use. As of January 2026, the following AI services have federal authorization:

AI Service	Authorization	Notes
Microsoft 365 Copilot	FedRAMP High (GCC, GCC-High, DoD)	Available Dec 2025; integrated with M365 apps
Azure OpenAI Service	FedRAMP High; IL4/IL5/IL6	GPT-4o, o1 series; Azure Government
Microsoft Copilot Studio	FedRAMP High (GCC/GCC-High)	Custom copilot/agent development
Google Gemini	FedRAMP (via Workspace)	Check current authorization level
Anthropic Claude	Via Palantir AIP (IL5)	On GSA Schedule; verify access path
C3 AI Platform	FedRAMP Moderate; IL5/IL6	Enterprise AI applications

Authorization status changes frequently. Always verify current authorization with your cybersecurity office before use. The table above reflects status as of January 2026 and may not reflect recent changes.

4.3.2 AI Tools List Maintenance

List Owner: Program Coordinator (or designated cybersecurity liaison)
Review Frequency: Quarterly, or when notified of authorization changes
Process:

1. Review FedRAMP marketplace and DoD authorization announcements

2. Verify current status of listed tools with cybersecurity office
3. Update table with additions, removals, or status changes
4. Distribute updated SOP to all trained developers
5. Log changes in document history

4.3.3 Approved Development Platforms

Platform	ATO Status	Typical Use
Microsoft Power Platform	Under M365 GCC ATO	Most applications
SharePoint Online	Under M365 GCC ATO	Data storage
Power BI	Under M365 GCC ATO	Dashboards

4.3.4 When Additional ATO Is Required

Additional Authority to Operate review is required when:

- Using platforms outside the approved list
- Connecting to external systems or APIs
- Processing data above platform's authorization level
- Deploying internet-facing applications

Contact cybersecurity office BEFORE development in these cases.

4.3.5 Security Controls for All Tools

All tools shall implement:

- **Authentication:** CAC/PIV or M365 authentication required
- **Authorization:** Role-based access controls
- **Audit Logging:** Track access and actions
- **Data Encryption:** At rest and in transit
- **Least Privilege:** Minimum necessary access

4.4 Operational Security (OPSEC)

Consider whether tools reveal unit strength, readiness, schedules, or operational patterns. Apply OPSEC principles during design. Consult unit OPSEC officer when uncertain.

4.5 Records Management

Tools creating federal records must comply with retention requirements. Identify record types, determine retention requirements, implement controls, and coordinate with Records Manager for new record types.

4.6 Incident Response

If a security incident occurs:

1. Immediately report to cybersecurity office
2. Preserve all logs and evidence
3. Disable tool access if directed
4. Cooperate fully with investigation

If something goes wrong: Report it, don't try to fix it quietly. Cybersecurity would rather help you early than clean up a mess later.

5. Development Prerequisites

5.1 Required

- Microsoft 365 Government account (GCC or GCC-High)
- Access to approved AI tools (per Section 4)
- Domain expertise in the problem area
- Completion of AI-Fluent Development Orientation (2 hours)
- Supervisor approval for development effort

5.2 Not Required

- Programming experience
- Software development background
- IT certifications

5.3 Obtaining Required Access

5.3.1 Microsoft 365 and Power Platform

Most DoD personnel already have M365 accounts. To verify and obtain Power Platform access:

1. **Check current access:** Navigate to `make.powerapps.com` with your CAC. If you can log in, you have basic access.
2. **If access denied:** Contact your unit S-6/G-6 or IT help desk to request Power Platform licensing.
3. **License tiers:**
    - **M365 E3/G3:** Includes Power Apps for Office 365, Power Automate, basic Power BI
    - **M365 E5/G5:** Includes advanced Power BI Pro features

- **Power Platform standalone:** May be required for premium connectors

4. **SharePoint site:** If you need a new SharePoint site for your tools, request through your SharePoint administrator or S-6.

5.3.2 AI Tool Access

Important: The prompts in the Training Curricula require conversational AI capable of generating code and iterating on solutions. Not all AI tools are equal—verify your tool can handle development tasks before beginning.

Recommended AI tools for EDD (in order of accessibility):

Tool	How to Obtain	Notes
Microsoft 365 Copilot	Unit license allocation; request through S-6	Best integration with Power Platform; may have limited availability
Azure OpenAI (via Azure Gov)	Request Azure Gov subscription through MSS Data Portal (`mss.data.mil`)	Most capable for complex development; requires Azure familiarity
Anthropic Claude (via Palantir AIP)	Command must have Palantir AIP contract	Excellent for iterative development; limited availability
Google Gemini (via Workspace)	Included with some Google Workspace Gov accounts	Check with IT if available

If you don't have AI access:

1. Check if your unit has M365 Copilot licenses available—ask S-6
2. Request Azure Government access via `https://mss.data.mil` (MSS Data Portal)
3. Coordinate with Program Coordinator to identify available options at your command
4. As interim solution: Commercial AI tools (ChatGPT, Claude.ai) may be used for learning/prototyping with synthetic data only—never input real PII, operational data, or government information

Minimum AI capability required: The AI must be able to (1) understand natural language descriptions of software requirements, (2) generate Power Apps formulas and Power Automate flow configurations, and (3) iterate based on error messages. Basic M365 Copilot in Power Apps meets these requirements for most tasks.

6. Development Workflow

6.1 Phase 1: Problem Definition (2–4 hours)

Define what you're building, why, and for whom. Complete Problem Definition Document (Appendix A). Obtain supervisor approval before proceeding.

6.2 Phase 2: Compliance Review (1–4 hours)

Complete Compliance Checklist (Appendix E). Determine PII/PHI involvement. Complete PIA Threshold Analysis if applicable. Verify tools and platforms are approved. Obtain required approvals before proceeding.

6.3 Phase 3: Rapid Prototyping (8–20 hours)

Build working solution through iterative development: Describe → Generate → Review → Test → Iterate.

Key principles:

- Never deploy code you cannot explain
- Small iterations beat large builds
- Test with real users early
- Save working versions before major changes

6.4 Phase 4: User Testing (4–8 hours)

Minimum 3 users test without developer assistance. Document feedback. Resolve critical issues before proceeding.

6.5 Phase 5: Documentation (First Tool: 20–40 hours; Subsequent: 8–16 hours)

Why this matters: Good documentation is what separates a useful tool from a burden you leave behind. Budget the time—your successor will thank you.
Reality check: Your first tool's documentation will take longer than estimated. This is normal. You're learning the documentation process while doing it. Subsequent tools go faster as you reuse templates and understand what's essential.

Required documentation package:

1. **User Guide** (2–5 pages): How to use the tool
2. **Replication Guide** (10–30 pages): How to rebuild from scratch
3. **Adaptation Guide** (5–10 pages): How to modify for different contexts
4. **Maintenance Guide** (5–10 pages): How to fix common issues and perform updates

6.6 Phase 6: Quality Assurance Review (2–4 hours)

Submit to QA reviewer. Complete QA Checklist (Appendix B). Address revisions. Obtain written approval before deployment.

6.7 Phase 7: Deployment and Registration (1–2 hours)

Deploy to production. Announce to users. Register in Tool Registry (Appendix C). Establish feedback channel.

6.8 Phase 8: Sustainment (Ongoing)

Monitor for issues. Update documentation when changes occur. Execute proper turnover before PCS/PCA.

7. Roles and Responsibilities

Developer: Complete training, follow workflow, create documentation, maintain tool, execute turnover.

QA Reviewer: Review functionality, verify documentation, verify compliance, approve or return with feedback. Cannot review own work.

7.1 QA Reviewer Designation

QA reviewers must meet one of the following criteria:

- Completed all three EDD training courses, OR
- Have successfully deployed at least one tool under this SOP, OR
- Are designated by the Program Coordinator based on equivalent experience

For units with limited personnel: If no qualified peer reviewer is available, the Section Supervisor may serve as QA reviewer. Document this exception in the QA Checklist remarks.

Maintaining the QA Pool:

- Program Coordinator maintains list of qualified QA reviewers
- List updated when developers complete qualification criteria
- Minimum of 2 qualified reviewers should be maintained per command

Section Supervisor: Approve problem definitions, allocate time, track inventory, ensure turnover compliance.

7.2 Supervisor Orientation Requirement

Before approving any developer's first Problem Definition Document, supervisors must complete a 30-minute Supervisor Orientation covering:

- The Four-Layer Framework (what EDD is and isn't)
- Time allocation expectations (realistic hours for development + documentation)
- How to evaluate Problem Definition Documents for feasibility
- Their role in the workflow (approvals, QA review option, turnover tracking)
- Where to find help (Program Coordinator, this SOP, training curricula)

This orientation may be delivered by the Program Coordinator, a trained developer, or via self-study of designated materials. Completion is documented in the training records.

Program Coordinator: Maintain registry, coordinate training, share best practices, report metrics, maintain QA reviewer list, maintain AI tools authorization list.

Cybersecurity Office: Advise on approved tools, review ATO requirements, respond to incidents.

Privacy Officer: Review PIA analyses, determine when full PIA required, advise on PII handling.

8. Training Requirements

Required: AI-Fluent Development Orientation (2 hours)—Creator mindset, framework, workflow, compliance.

Recommended: Platform Training (4 hours)—Power Platform, SharePoint, Power Automate, Power BI.

Optional: Advanced Workshop (4 hours)—Complex projects, integrations, optimization.

Supervisor Orientation: (30 minutes)—Required for supervisors before approving development efforts.

See Training Curricula document for full course content and instructor requirements.

9. Metrics and Assessment

Tool-Level: User count, usage frequency, issues reported, estimated time saved, user satisfaction.

Program-Level: Tools deployed, developers trained, total impact, documentation compliance, turnover success.

Intellectual Honesty: Distinguish measured vs. estimated metrics. Document methodology. Do not overclaim.

10. Scaling and Adoption

10.1 90-Day Pilot Model

Weeks 1–2: Identify 3–5 interested personnel, conduct orientation, each identifies one problem.

Weeks 3–8: Build solutions using this SOP, weekly check-ins, peer collaboration.

Weeks 9–10: Complete documentation, QA review, compile lessons learned.

Weeks 11–12: Measure outcomes, gather feedback, decide: expand, modify, or discontinue.

10.2 Pilot Success Criteria

The pilot is successful if:

- At least 3 of 5 developers complete a working tool with documentation
- At least 2 tools show measurable usage (minimum 5 users or 20 uses in final 2 weeks)
- Documentation quality passes QA review without major revision cycles
- No security incidents occur
- Participant feedback is net positive (recommend continuing program)

10.3 Pilot Failure Criteria

Consider discontinuing or significantly modifying the pilot if:

- Fewer than 2 of 5 developers complete a working tool
- No tools achieve measurable usage
- Security or compliance incidents occur that weren't caught by the process

- Developer time investment exceeds estimates by more than 3x without corresponding value
- Majority of participants report they would not recommend the program

Failure isn't defeat: If the pilot fails, document why. Was it the methodology, the implementation, the personnel selection, or the timing? Lessons learned from failed pilots improve future attempts.

10.4 Tool Registry Implementation

The Tool Registry (Appendix C) may not exist at pilot start. Implementation options:

1. **Simple start:** SharePoint list with registry fields, created in Week 1
2. **Structured approach:** One pilot developer builds registry as their tool
3. **Manual interim:** Spreadsheet maintained by Program Coordinator until formal registry built

Registry requirements: searchable, accessible to all unit members, includes fields from Appendix C template.

10.5 Expansion Model

Trained developers become trainers. Each trains 3–5 more. Capability compounds organically. Central coordination maintains standards.

11. References

(a) DoD 5400.11-R, DoD Privacy Program

(b) DoDI 8510.01, Risk Management Framework for DoD IT

(c) SECNAVINST 5239.3C, DoN Cybersecurity Policy

(d) SECNAVINST 5211.5F, DoN Privacy Program

(e) MCO 5239.2B, Marine Corps Cybersecurity Program

(f) NIST SP 800-53, Security and Privacy Controls

A. Problem Definition Template

PROBLEM DEFINITION DOCUMENT

TOOL NAME: _____ **DATE:** _____
DEVELOPER: _____

1. PROBLEM STATEMENT (2–3 sentences)

_____

_____

2. TARGET USERS: _____ **ESTIMATED COUNT:** _____

3. SUCCESS CRITERIA (measurable)

- Metric 1: _____
- Metric 2: _____

4. REQUIRED FUNCTIONS (minimum viable)

1. _____
2. _____
3. _____

5. DATA CONSIDERATIONS
Will tool collect/store PII? ☐ Yes ☐ No
Will tool collect/store PHI? ☐ Yes ☐ No
If yes, describe controls: _____

6. PLATFORM: ☐ Power Platform ☐ Desktop ☐ Other: _____
7. ESTIMATED EFFORT: Development _____ hrs Documentation _____ hrs

DEVELOPER SIGNATURE: _____ **DATE:** _____
SUPERVISOR APPROVAL: _____ **DATE:** _____

B. QA Review Checklist

QA REVIEW CHECKLIST

TOOL NAME: _____ **DATE:** _____
DEVELOPER: _____
REVIEWER: _____
Reviewer Qualification: ☐ Completed all training ☐ Deployed tool ☐ Coordinator designated ☐ Supervisor (exception)

FUNCTIONALITY	**Pass/Fail**
☐ All stated functions work as intended	_____
☐ Error states handled gracefully	_____
☐ User interface is intuitive	_____
☐ Performance acceptable	_____
USER TESTING	
☐ Minimum 3 users tested without developer assistance	_____
☐ Critical feedback addressed	_____
DOCUMENTATION	
☐ User Guide complete	_____
☐ Replication Guide complete	_____
☐ Adaptation Guide complete	_____
☐ Maintenance Guide complete	_____
COMPLIANCE	
☐ No unauthorized PII	_____
☐ No unauthorized PHI	_____
☐ Approved platform used	_____
☐ Security controls implemented	_____
☐ PIA completed (if required)	_____
TURNOVER READINESS	
☐ Tool registered in inventory	_____
☐ Maintainer designated	_____
☐ Documentation accessible to successor	_____

RESULT: ☐ APPROVED ☐ REVISIONS REQUIRED
REQUIRED REVISIONS: _____

REVIEWER SIGNATURE: _____ **DATE:** _____

C. Tool Registry Entry

TOOL REGISTRY ENTRY

Tool Name: _____ **Version:** _____
Developer: _____ **Deploy Date:** _____
Platform: _____

Description:

Target Users: _____ **User Count:** _____
Documentation Location: _____
Current Maintainer: _____
Maintainer Contact: _____

Status: ☐ Active ☐ Deprecated ☐ Under Revision
Data Sensitivity: ☐ No PII ☐ PII (controlled)
Last Review: _____ **Next Review:** _____
Notes: _____

D. PIA Threshold Analysis

PRIVACY IMPACT ASSESSMENT THRESHOLD ANALYSIS

TOOL NAME: _____ **DATE:** _____
DEVELOPER: _____

Answer each question. If ANY answer is YES, coordinate with Privacy Officer.

	Yes	No
1. Will the tool collect PII from individuals?	☐	☐
2. If yes, will it collect from 10+ individuals?	☐	☐
3. Will the tool create a new database containing PII?	☐	☐
4. Will PII be retrievable by individual identifier?	☐	☐
5. Will the tool share PII with external parties?	☐	☐
6. Will the tool use PII for a new purpose?	☐	☐
7. Will the tool collect PII about minors?	☐	☐

If ALL answers are NO: Document this analysis and proceed with development.
If ANY answer is YES: Coordinate with Privacy Officer before proceeding.

Privacy Officer: _____ **Phone:** _____

DEVELOPER SIGNATURE: _____ **DATE:** _____

E. Compliance Checklist

COMPLIANCE CHECKLIST

TOOL NAME: _____ **DATE:** _____
DEVELOPER: _____

DATA CLASSIFICATION
☐ Confirmed: No classified data involved
☐ Confirmed: No CUI unless platform authorized
☐ PII assessment complete (see PIA Threshold Analysis)
☐ PHI assessment complete (N/A or coordinated with medical)

AI TOOLS
☐ AI tool(s) verified as approved for government use
☐ Tool(s) used: _____

PLATFORM
☐ Development platform is pre-authorized, OR
☐ Additional ATO obtained (attach documentation)

SECURITY CONTROLS
☐ Authentication required (CAC/M365)
☐ Role-based access controls implemented
☐ Audit logging enabled
☐ Data encrypted at rest and in transit

OPSEC
☐ Reviewed for operational security concerns
☐ No sensitive operational patterns revealed

RECORDS MANAGEMENT
☐ Record types identified
☐ Retention requirements determined
☐ N/A—tool does not create federal records

ADDITIONAL APPROVALS NEEDED
☐ None beyond standard workflow
☐ Privacy Officer review required
☐ Cybersecurity review required
☐ Legal review required
☐ Other: _____

DEVELOPER SIGNATURE: _____ **DATE:** _____
REVIEWER SIGNATURE: _____ **DATE:** _____

UNCLASSIFIED // Distribution Unlimited
Version 3.0 — 26 January 2026