Standard Operating Procedure

Expert-Driven AI-Assisted Development

A Methodology for Building Institutional Capability

Document Version: 5.0
Effective Date: February 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 **4**
- 1.1 Purpose 4
- 1.2 EDD IS / EDD ISN'T 4
- 1.3 Scope 4
- 1.4 Applicability 4

2 The Four-Layer Framework **4**
- 2.1 Layer 1: Direct Tool Development 4
- 2.2 Layer 2: Process Liberation 5
- 2.3 Layer 3: Capability Cultivation 5
- 2.4 Layer 4: Documentation and Replication 5

3 The Creator Mindset **5**
- 3.1 Consumer vs Creator 5
- 3.2 The Artifact Test 6

4 Compliance and Security **6**
- 4.1 Data Classification 6
- 4.2 Privacy Requirements 6
- 4.3 Cybersecurity 7
- 4.4 OPSEC 8
- 4.5 Records Management 8
- 4.6 Incident Response 8

5 Development Prerequisites **9**
- 5.1 Required 9
- 5.2 Not Required 9
- 5.3 Obtaining Access 9

6 Development Workflow **10**
- 6.1 Phase 1: Problem Definition 10
- 6.2 Phase 2: Compliance Review 10
- 6.3 Phase 3: Rapid Prototyping 10
- 6.4 Phase 4: User Testing 10
- 6.5 Phase 5: Documentation 10
- 6.6 Phase 6: QA Review 11
- 6.7 Phase 7: Deployment 11
- 6.8 Phase 8: Sustainment 11

7 Roles and Responsibilities **11**
- 7.1 Developer 11
- 7.2 QA Reviewer 11
- 7.3 Supervisor 12
- 7.4 Program Coordinator 12
- 7.5 Cybersecurity Office 12
- 7.6 Privacy Officer 12

8 Training Requirements **12**
8.1 Required 12
8.2 Recommended for Builders 12
8.3 Recommended for Leadership 13
8.4 Six 201-Level Skills 13
8.5 Instructor Certification 13

9 Metrics and Assessment **14**
9.1 Tool-Level Metrics 14
9.2 Program-Level Metrics 14

10 Scaling and Adoption **15**
10.1 90-Day Pilot Model 15
10.2 Success / Failure Criteria 15
10.3 Tool Registry 15
10.4 Expansion Model 16

11 References **16**
11.1 Policy and Regulatory References 16
11.2 Research Foundation 16

12 Appendices **17**

A Problem Definition Template **18**

B QA Review Checklist **19**

C Tool Registry Entry **20**

D PIA Threshold Analysis **21**

E Compliance Checklist **22**

1. Purpose and Scope

1.1 Purpose

This Standard Operating Procedure establishes the framework, governance, and workflow for AI-assisted tool development by subject-matter experts within Department of War (DoW) organizations. Expert-Driven Development enables domain experts to build, document, and sustain institutional tools using AI as a development accelerator—without requiring a background in software engineering, contracting, or formal IT acquisition.

1.2 EDD IS / EDD ISN'T

EDD IS

- A framework for building institutional tools using AI
- A way to turn subject-matter expertise into working software
- A governance model for responsible AI-assisted development
- A training pipeline that produces AI-fluent builders
- A documentation standard that ensures tool continuity
- Compatible with existing DoW cybersecurity and privacy requirements

EDD ISN'T

- A replacement for professional software development or IT acquisition
- An authorization to bypass cybersecurity or privacy controls
- A way to build systems that handle classified data
- A shortcut that eliminates the need for documentation
- A single AI tool or platform
- Limited to any specific programming language or technology stack

1.3 Scope

This SOP covers the complete lifecycle of AI-assisted tool development: from problem identification and compliance review through prototyping, testing, documentation, deployment, and sustainment. It applies to tools built on approved platforms using approved AI assistants that handle unclassified data only.

1.4 Applicability

This SOP applies to all personnel who develop, review, supervise, or maintain tools built using the Expert-Driven Development framework. It is designed for adoption at the unit level and can be tailored to organization-specific requirements while maintaining compliance with DoW-wide cybersecurity and privacy directives.

2. The Four-Layer Framework

Expert-Driven Development operates through four interdependent layers. Each layer builds on the previous one, and all four must be present for the framework to produce sustainable results.

2.1 Layer 1: Direct Tool Development

Subject-matter experts use AI to build tools that solve real problems in their organizations. The expert provides domain knowledge—the understanding of the problem, the workflow, the users, and

the requirements. AI provides the development capability—translating that domain knowledge into working code, interfaces, and automation.

Key Principle

The expert drives the development. AI is the accelerator, not the decision-maker. Every design choice, workflow decision, and feature prioritization comes from the person who understands the problem.

2.2 Layer 2: Process Liberation

By removing the dependency on contractors, acquisition timelines, and IT development queues, EDD liberates the development process. Personnel can identify a problem and begin building a solution within the same week—not the same fiscal year. This layer addresses the structural bottleneck that prevents organizations from responding to their own needs.

2.3 Layer 3: Capability Cultivation

Each build develops the builder. The five-course training curriculum and the 201-level skills framework cultivate six core competencies: Context Assembly, Quality Judgment, Task Decomposition, Iterative Refinement, Workflow Integration, and Frontier Recognition. Personnel who complete EDD projects gain transferable skills in AI-assisted development, systems thinking, user-centered design, and technical documentation. These capabilities persist after the specific tool is deployed and compound across subsequent projects.

2.4 Layer 4: Documentation and Replication

Every tool built under EDD is documented to a standard that enables another person to understand, maintain, modify, and replicate the tool without the original builder present. This layer ensures that institutional knowledge does not walk out the door when personnel transfer. Documentation is not an afterthought—it is a core deliverable of every project.

3. The Creator Mindset

EDD requires a fundamental shift in how personnel interact with AI tools. Most users operate as consumers—they use AI to get answers, summarize text, or draft emails. EDD trains personnel to operate as creators—using AI to build things that other people use.

3.1 Consumer vs Creator

Dimension	Consumer	Creator
Output	Answers for yourself	Tools for others
Interaction	Single prompt, single response	Iterative conversation toward a build
Scope	Personal productivity	Institutional capability
Duration	One-time use	Persistent, maintained artifact

Dimension	Consumer	Creator
Accountability	None—private use	Documented, reviewed, and sustained
Knowledge transfer	None	Documentation package enables replication

3.2 The Artifact Test

The simplest way to determine whether someone is operating as a consumer or a creator:

> ***Does your AI interaction produce an artifact that someone else can use?***
>
> *If the answer is yes—a tool, an application, a system, a workflow—you are creating. If the answer is no—a summary, an email draft, a personal answer—you are consuming. Both are valid. EDD focuses on creating.*

4. Compliance and Security

All development under this SOP must comply with existing DoW cybersecurity, privacy, OPSEC, and records management requirements. AI-assisted development does not create new exceptions to these requirements—it operates within them.

4.1 Data Classification

EDD tools handle **unclassified data only**. The following data types are prohibited from use in AI-assisted development:

Prohibited Data

- Classified information (any level)
- Controlled Unclassified Information (CUI) unless the platform is CUI-authorized
- Personally Identifiable Information (PII) unless a Privacy Impact Assessment has been completed
- Protected Health Information (PHI)
- For Official Use Only (FOUO) data in non-authorized environments
- Operational plans, force movement data, or intelligence products

4.2 Privacy Requirements

Tools that collect, store, process, or display information about individuals must comply with DoW privacy directives. The following apply:

4.2.1 Privacy Impact Assessment (PIA)

Required for any tool that collects or maintains PII. A PIA threshold analysis must be completed during the Compliance Review phase (Phase 2) to determine whether a full PIA is required.

4.2.2 System of Records Notice (SORN)

If the tool creates a new system of records retrievable by a personal identifier, a SORN must be published in the Federal Register before the tool goes into production use.

4.2.3 Appeals and Redress

Any tool that makes decisions affecting individuals must include a mechanism for individuals to review, contest, and correct information about themselves.

4.3 Cybersecurity

4.3.1 Approved AI Tools

The following AI tools are approved for use in EDD development. Authorization levels indicate the scope of approved use:

Tool	Authorization Level	Notes
M365 Copilot	Enterprise-authorized	Available through existing DoW M365 licensing; data stays within tenant
Azure OpenAI	Enterprise-authorized	Requires Azure Government subscription; FedRAMP High authorized
Copilot Studio	Enterprise-authorized	Low-code bot builder within M365 ecosystem
Gemini	Approved with restrictions	Unclassified use only; do not input PII or CUI
Claude	Approved with restrictions	Unclassified use only; do not input PII or CUI
C3 AI	Enterprise-authorized	DoW Enterprise AI platform; available through enterprise agreement

4.3.2 Approved Platforms

Tools built under EDD must be deployed on approved platforms:

Platform	Use Case	Authorization
Microsoft Power Platform	Low-code applications, automation, dashboards	Enterprise-authorized within DoW M365
SharePoint Online	Web-based tools, document management, portals	Enterprise-authorized within DoW M365
Azure Government	Cloud-hosted applications, APIs, databases	FedRAMP High; requires subscription
GitHub (public)	Open-source projects, static sites, documentation	Unclassified public release only

4.3.3 When an ATO Is Required

An Authority to Operate (ATO) is required when a tool:

- Connects to or operates on the DoW Information Network (DoWIN)
- Processes, stores, or transmits CUI
- Integrates with other authorized information systems
- Operates outside the inherited authorization boundary of its host platform

Tools built entirely within the inherited authorization boundary of an approved platform (e.g., a Power App within DoW M365) typically do not require a separate ATO but must still comply with the platform's security controls.

4.3.4 Security Controls

All tools must implement security controls appropriate to their data sensitivity and deployment environment, including:

- Authentication via CAC or enterprise identity provider
- Role-based access control (RBAC) where applicable
- Audit logging of user actions and data access
- Input validation and output encoding
- Encryption of data in transit (TLS 1.2+) and at rest

4.4 OPSEC

Developers must apply OPSEC principles throughout the development lifecycle. Do not include operational details, unit-specific procedures, force structure information, or vulnerability assessments in AI prompts, tool documentation, or publicly accessible code repositories. When in doubt, consult your organization's OPSEC officer before proceeding.

4.5 Records Management

Development artifacts (documentation packages, source code, deployment records) are official records and must be managed in accordance with DoW records management directives. Retain all project documentation for the duration specified by the applicable records schedule. The documentation package produced in Phase 5 serves as the primary record of each development effort.

4.6 Incident Response

If a security incident occurs involving an EDD tool (data breach, unauthorized access, malware, or compromise of an AI tool), personnel must:

1. Immediately cease use of the affected tool
2. Report the incident to the organization's Cybersecurity Office within 1 hour
3. Preserve all logs, artifacts, and evidence related to the incident
4. Notify the chain of command and the EDD Program Coordinator
5. Cooperate with the incident response investigation
6. Do not attempt to remediate the vulnerability without authorization

5. Development Prerequisites

5.1 Required

- Completed EDD training (minimum: AI Fluency Fundamentals)
- Supervisor approval for the specific development project
- Access to at least one approved AI tool
- Access to at least one approved deployment platform
- A defined problem that meets the criteria in Phase 1
- Completed Problem Definition Template

5.2 Not Required

- A background in software engineering or computer science
- Prior programming experience
- A contract, funding, or acquisition document
- An IT service request or development ticket
- Permission from a centralized IT authority (unless ATO is required)

5.3 Obtaining Access

5.3.1 Microsoft 365

Most DoW personnel already have M365 accounts. Power Platform access may require a license assignment through your organization's M365 administrator. Contact your local IT support to verify your license includes Power Apps, Power Automate, and Copilot Studio.

5.3.2 AI Tools

The following table provides recommendations for obtaining access to approved AI tools:

Tool	How to Obtain Access	Recommendation
M365 Copilot	Enterprise license assignment through M365 admin	Start here if your organization has Copilot licenses
Azure OpenAI	Azure Government subscription; request through cloud team	Best for custom API-driven development
Copilot Studio	Included with Power Platform licensing	Best for building conversational AI assistants
Gemini	Web access at gemini.google.com (unclassified only)	Good general-purpose coding assistant
Claude	Web access at claude.ai (unclassified only)	Strong for complex reasoning and documentation
C3 AI	Enterprise agreement; contact your AI/ML program office	Best for data-heavy enterprise applications

6. Development Workflow

The EDD development workflow consists of eight phases. Each phase has defined inputs, outputs, and time estimates. Phases are sequential, but iteration between adjacent phases is expected and encouraged.

6.1 Phase 1: Problem Definition

Estimated time: 2–4 hours

Identify and document the problem you intend to solve. Complete the Problem Definition Template. Define the current state, desired state, affected users, and success criteria. A well-defined problem is the single strongest predictor of a successful build.

Output: Completed Problem Definition Template.

6.2 Phase 2: Compliance Review

Estimated time: 1–4 hours

Review the proposed tool against compliance requirements. Complete the Compliance Checklist. Determine data classification, privacy requirements, and whether an ATO is needed. Identify the appropriate deployment platform. Obtain supervisor approval to proceed.

Output: Completed Compliance Checklist with supervisor signature.

6.3 Phase 3: Rapid Prototyping

Estimated time: 8–20 hours

Build the tool using AI-assisted development. Start with the minimum viable feature set identified in Phase 1. Use iterative prompting to develop, test, and refine functionality. Maintain a development journal documenting key decisions, prompts that worked, and problems encountered.

Output: Working prototype with core functionality.

6.4 Phase 4: User Testing

Estimated time: 4–8 hours

Put the prototype in front of actual users. Observe how they interact with it. Collect feedback on usability, functionality, and missing features. Iterate on the prototype based on user feedback. A minimum of three users should test the tool before proceeding to documentation.

Output: User-tested prototype with documented feedback and revisions.

6.5 Phase 5: Documentation

Estimated time: 20–40 hours (first project) / 8–16 hours (subsequent)

Produce the documentation package. This is the most critical phase for institutional value. The documentation must enable someone who has never seen the tool to understand what it does, how it works, how to maintain it, how to modify it, and how to replicate it. First-time builders

should expect to spend significantly more time on documentation; the investment decreases with experience.

Output: Complete documentation package.

6.6 Phase 6: QA Review

Estimated time: 2–4 hours

A designated QA Reviewer examines the tool and its documentation against the QA Checklist. The reviewer verifies functionality, security compliance, documentation completeness, and readiness for deployment. The reviewer must not be the same person who built the tool.

Output: Completed QA Checklist with reviewer sign-off or remediation requirements.

6.7 Phase 7: Deployment

Estimated time: 1–2 hours

Deploy the tool to its production environment. Register the tool in the Tool Registry. Communicate availability to intended users. Establish the sustainment plan, including who is responsible for ongoing maintenance and how issues will be reported and resolved.

Output: Deployed tool, completed Tool Registry entry, and sustainment plan.

6.8 Phase 8: Sustainment

Estimated time: Ongoing

Maintain the tool in its operational environment. Monitor usage metrics, address user-reported issues, apply updates as needed, and update documentation to reflect changes. Plan for turnover: when the original builder departs, the documentation package must be sufficient for a successor to assume maintenance responsibility.

Output: Operational tool with current documentation and identified maintainer.

7. Roles and Responsibilities

7.1 Developer

The individual who builds the tool. Responsible for completing all eight phases of the development workflow, maintaining compliance with this SOP, producing the documentation package, and sustaining the tool through its operational lifecycle. Any personnel member who has completed the required training and received supervisor approval may serve as a developer.

7.2 QA Reviewer

The individual who reviews the tool and documentation in Phase 6. The QA Reviewer must be a different person from the developer. Designation criteria:

- Has completed EDD training (minimum: AI Fluency Fundamentals)
- Has built at least one tool under EDD, or has been designated by the Program Coordinator
- Is familiar with the compliance requirements in Section 4

- Has no conflict of interest with the tool being reviewed

7.3 Supervisor

The developer's direct supervisor. Responsible for approving the development project, allocating duty time for development, and ensuring the tool meets organizational needs. Supervisors are required to complete the Supervisor Orientation before approving their first EDD project. This orientation ensures supervisors understand the framework, can evaluate proposals, and know what good AI-assisted output looks like.

7.4 Program Coordinator

The individual responsible for managing the EDD program at the organizational level. Maintains the Tool Registry, designates QA Reviewers, coordinates training, tracks program metrics, and reports program status to leadership. The Program Coordinator may also serve as a developer or QA Reviewer.

7.5 Cybersecurity Office

The organization's cybersecurity team. Provides guidance on security controls, reviews ATO requirements, responds to security incidents involving EDD tools, and validates that tools comply with cybersecurity directives. Consulted during Phase 2 (Compliance Review) for any tool that connects to the network or processes sensitive data.

7.6 Privacy Officer

The organization's designated privacy official. Reviews PIA threshold analyses, advises on SORN requirements, and ensures tools that handle PII comply with DoW privacy directives. Consulted during Phase 2 for any tool that collects, stores, or displays information about individuals.

8. Training Requirements

The v5 curriculum comprises five courses organized by audience and prerequisite chain.

8.1 Required

The following course is the universal prerequisite and must be completed before beginning any EDD activity:

Course	Audience	Duration	Prerequisite
AI Fluency Fundamentals	All personnel	2 hours	None (universal prerequisite)

8.2 Recommended for Builders

The following courses are recommended/elective for personnel who will build tools:

Course	Audience	Duration	Prerequisite
Builder Orientation	Aspiring builders	2 hours	AI Fluency Fundamentals
Platform Training	Builders	4 hours	Builder Orientation
Advanced Workshop	Experienced builders	4 hours	At least one deployed tool

8.3 Recommended for Leadership

The following course is recommended for supervisors and leadership personnel:

Course	Audience	Duration	Prerequisite
Supervisor Orientation	Supervisors approving EDD projects	30 minutes	None

8.4 Six 201-Level Skills

The training curriculum develops six core competencies defined in the 201-level skills framework. These skills represent the capabilities that separate effective AI-assisted builders from casual AI users:

1. **Context Assembly**—The ability to gather and structure the right information so AI can produce useful output.
2. **Quality Judgment**—The ability to evaluate AI-generated output for correctness, completeness, and fitness for purpose.
3. **Task Decomposition**—The ability to break complex problems into discrete, AI-addressable tasks.
4. **Iterative Refinement**—The ability to systematically improve AI output through structured feedback cycles.
5. **Workflow Integration**—The ability to embed AI-assisted processes into existing organizational workflows.
6. **Frontier Recognition**—The ability to identify where AI capability boundaries lie and adjust approach accordingly.

8.5 Instructor Certification

Instructors for each course must meet the following certification requirements:

Course	Requirements
AI Fluency Fundamentals	Completed course AND at least one builder course
Builder Orientation	Completed all builder courses AND deployed at least one tool
Platform Training	Completed all builder courses, deployed at least one tool, plus Power Platform proficiency

Course	Requirements
Advanced Workshop	Completed all builder courses, deployed at least one tool, plus served as QA reviewer for 2+ tools
Supervisor Orientation	Any qualified AI Fluency Fundamentals instructor

Certification process: Complete course as student → Build/deploy tool → Shadow instructor → Co-teach → Certification from Program Coordinator.

9. Metrics and Assessment

Metrics serve two purposes: demonstrating the value of individual tools and assessing the health of the overall EDD program. All metrics should be collected consistently and reported to leadership quarterly.

9.1 Tool-Level Metrics

Collected for each deployed tool:

Metric	What It Measures	Collection Method
Active users	Adoption and utility	Platform analytics or usage logs
Time saved per use	Efficiency gain	User survey or workflow comparison
Error rate reduction	Quality improvement	Before/after error tracking
Build time	Development efficiency	Developer-reported hours
Development cost	Cost avoidance	Hours multiplied by composite labor rate
User satisfaction	Quality of the solution	Post-deployment survey

9.2 Program-Level Metrics

Collected across all EDD activity within the organization:

Metric	What It Measures	Target
Number of trained personnel	Pipeline capacity	Growing quarter-over-quarter
Number of deployed tools	Program output	Growing quarter-over-quarter
Completion rate (started vs deployed)	Process effectiveness	>70% of started projects reach deployment

Metric	What It Measures	Target
Documentation compliance rate	Quality assurance	100% of deployed tools have complete packages
Total estimated cost avoidance	Return on investment	Reported quarterly to leadership
Security incidents	Risk management	Zero incidents per quarter

10. Scaling and Adoption

10.1 90-Day Pilot Model

Organizations adopting EDD should begin with a 90-day pilot. The pilot provides a controlled environment to validate the framework, train initial personnel, produce the first tools, and establish organizational processes before expanding.

Phase	Timeline	Activities
Setup	Days 1–14	Designate Program Coordinator, identify 2–4 pilot developers, conduct training, verify platform access
First builds	Days 15–60	Pilot developers complete Phases 1–5 on their first projects with coaching support
QA and deployment	Days 61–75	QA reviews, remediation, deployment, and Tool Registry entries
Assessment	Days 76–90	Collect metrics, brief leadership, decide on expansion

10.2 Success / Failure Criteria

Success Criteria

- At least 2 tools deployed and in active use
- All deployed tools have complete documentation packages
- Zero security incidents during the pilot
- Measurable time savings or error reduction demonstrated
- Leadership endorsement for expansion

Failure Indicators

- No tools reach deployment within 90 days
- Security or compliance violations occur
- Developers cannot obtain platform access
- Leadership does not allocate duty time for development
- Documentation requirements are waived or ignored

10.3 Tool Registry

The Tool Registry is a centralized record of all tools built under EDD within the organization. Every deployed tool must have an entry. The registry tracks:

- Tool name and description

- Developer and current maintainer
- Deployment platform and URL
- Data classification
- User count and status (active, deprecated, retired)
- Documentation package location
- Date deployed and last updated

The Program Coordinator maintains the Tool Registry and reviews it monthly to identify tools that need updates, lack a maintainer, or should be retired.

10.4 Expansion Model

After a successful pilot, expansion follows a train-the-trainer model:

1. Pilot developers become QA Reviewers and mentors for the next cohort
2. Each cohort is 2–4 new developers with defined projects
3. New cohorts begin every 60–90 days
4. The Program Coordinator scales training, QA capacity, and registry management as the program grows
5. Cross-organizational sharing is encouraged through the Tool Registry and documentation standards

11. References

11.1 Policy and Regulatory References

- DoW Directive 8140.01—Cyberspace Workforce Management
- DoW Instruction 5000.87—Operation of the Software Acquisition Pathway
- DoW Instruction 5200.48—Controlled Unclassified Information (CUI)
- DoW Instruction 5400.11—DoW Privacy and Civil Liberties Programs
- DoW Instruction 8500.01—Cybersecurity
- DoW Instruction 8510.01—Risk Management Framework (RMF) for DoW Systems
- DoW Instruction 8582.01—Security of Non-DoW Information Systems
- DoW Directive 3020.26—Department of War Continuity Policy
- DoWM 5200.01—DoW Information Security Program
- SECNAV M-5210.1—Department of the Navy Records Management Program
- NIST SP 800-53 Rev. 5—Security and Privacy Controls for Information Systems and Organizations
- OMB Circular A-130—Managing Information as a Strategic Resource
- Executive Order 14110—Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
- DoW AI Strategy, January 2026

11.2 Research Foundation

- Dell'Acqua, F., et al. (2023). "Navigating the Jagged Technological Frontier." Harvard Business School / BCG. Study of 758 consultants demonstrating the jagged frontier of AI capability.
- Brynjolfsson, E., Li, D., & Raymond, L. (2025). "Generative AI at Work." Stanford / MIT. Study of 5,172 customer-support agents demonstrating skill-leveling effects of AI assistance.

- Mollick, E. (2026). "Management as AI Superpower." Wharton School. Research on the delegation equation and management capabilities in AI-assisted work.
- OpenAI (2025). "GDPval: Measuring Economic Value of AI." Study of 1,320 tasks establishing expert parity benchmarks.
- UK Government Digital Services (2025). AI-assisted development deployment across 20,000 employees, demonstrating government-scale deployment patterns.
- Microsoft Work Trend Index. Study of 300,000+ employees identifying 80% tool abandonment rate without structured training.
- Stanford Digital Economy Lab. Research on the apprenticeship crisis and implications for AI-assisted skill development.

12. Appendices

The following templates are used throughout the EDD development workflow. Download each template and complete it during the appropriate phase.

Template	**Used In**	**Filename**
Problem Definition Template	Phase 1: Problem Definition	problem-definition.md
QA Checklist	Phase 6: QA Review	qa-checklist.md
Tool Registry Entry	Phase 7: Deployment	tool-registry-entry.md
PIA Threshold Analysis	Phase 2: Compliance Review	documentation-package-outline.md
Compliance Checklist	Phase 2: Compliance Review	development-journal.md

A. Problem Definition Template

Field	Entry
Tool Name	_____
Developer Name	_____
Date	_____
Organization	_____
Problem Statement	Describe the problem in 2–3 sentences. What is happening now that is inefficient, error-prone, or unsustainable?
Current State	How is this task currently performed? What tools are used? How long does it take?
Desired State	What does the ideal workflow look like after the tool is deployed?
Affected Users	Who will use this tool? How many users? What are their roles?
Success Criteria	How will you know the tool works? Define 2–3 measurable outcomes.
Data Requirements	What data will the tool process? What is the classification level? Does it include PII?
Deployment Platform	Where will the tool be hosted? (e.g., SharePoint, Power Platform, Azure)
Estimated Timeline	How many hours/days do you expect to invest in Phases 1–7?
Supervisor Approval	Name, rank, signature, date

B. QA Review Checklist

#	Item	Pass/Fail Notes
Functionality		
1	Tool performs all functions described in the Problem Definition Template	
2	All user-facing features work without errors	
3	Edge cases and error conditions are handled gracefully	
Security & Compliance		
4	Tool handles only unclassified data	
5	No PII is processed without a completed PIA	
6	Authentication and access controls are implemented	
7	Compliance Checklist is complete and signed	
Documentation		
8	Documentation package is complete	
9	A new person could maintain the tool using only the documentation	
10	User guide is clear and accurate	
11	Technical documentation describes architecture and dependencies	
Deployment Readiness		
12	Tool is deployed on an approved platform	
13	Sustainment plan identifies a maintainer	
14	Tool Registry entry is complete	

Reviewer Name / Signature:	_____
Date:	_____
Recommendation:	Approve Remediate

C. Tool Registry Entry

Field	**Entry**
Tool Name	_____
Description	Brief description of what the tool does (1–2 sentences)
Developer	Name, rank, organization
Current Maintainer	Name, rank, organization
Deployment Platform	(e.g., SharePoint, Power Platform, Azure, GitHub)
URL / Location	_____
Data Classification	(e.g., Unclassified, CUI)
PII Handled	Yes / No
ATO Required	Yes / No
User Count	_____
Status	Active / Deprecated / Retired
Date Deployed	_____
Last Updated	_____
Documentation Location	Path or URL to the documentation package
Sustainment Plan	Who maintains it and how issues are reported

D. PIA Threshold Analysis

Complete this analysis during Phase 2 (Compliance Review) for every tool. If any answer in Section 2 is "Yes," consult the Privacy Officer to determine whether a full PIA is required.

#	Question	Yes / No
Section 1: System Description		
1	What is the name of the tool?	_____
2	What is the purpose of the tool?	_____
3	Who are the intended users?	_____
Section 2: PII Determination		
4	Does the tool collect, store, or display names of individuals?	
5	Does the tool collect, store, or display Social Security Numbers or DoD ID Numbers?	
6	Does the tool collect, store, or display contact information (email, phone, address)?	
7	Does the tool collect, store, or display personnel records or performance data?	
8	Does the tool collect, store, or display medical or health information?	
9	Does the tool collect, store, or display financial information?	
10	Does the tool make decisions that affect individuals (assignments, evaluations, access)?	
Section 3: Determination		
If all answers in Section 2 are "No":		Full PIA not required
If any answer in Section 2 is "Yes":		Consult Privacy Officer
Analyst Name / Signature:		_____
Date:		_____

E. Compliance Checklist

Complete this checklist during Phase 2 (Compliance Review) before beginning development.

#	Item	Status	Notes
Data Classification			
1	Tool processes only unclassified data		
2	No CUI will be processed (or platform is CUI-authorized)		
3	No classified data will be processed at any level		
Privacy			
4	PIA Threshold Analysis completed (Appendix D)		
5	Privacy Officer consulted (if PII is involved)		
6	SORN requirements reviewed (if applicable)		
Cybersecurity			
7	Tool will be deployed on an approved platform		
8	AI tools used are on the approved list		
9	ATO requirement determined (required / not required)		
10	Cybersecurity Office consulted (if connecting to DoWIN)		
OPSEC			
11	No operational details in AI prompts or code		
12	No force structure or vulnerability data exposed		
Records Management			
13	Records retention schedule identified		
14	Documentation will be stored in an approved location		
Approval			
Developer Name / Signature:		_____	
Supervisor Name / Signature:		_____	
Date:		_____	