White Papers & Template

When are white papers required or suggested and how are they used and evaluated?

In the military ecosystem, white papers are the definitive "gatekeeper" documents used to filter ideas, technologies, and policies before they consume significant time, funding, or bureaucratic momentum.

Military innovation hubs (such as AFWERX or the Army Applications Laboratory), acquisition agencies, and commanding officers use white papers to determine whether a concept warrants a formal, multi-million-dollar proposal.

1. When are White Papers Required or Suggested?

The military utilizes white papers across distinct operational and acquisition phases:

Required Scenarios (Mandatory Gates)

- **Two-Step Broad Agency Announcements (BAAs):** To save time for both vendors and the government, agencies like DARPA or service-branch labs mandate a white paper as **Step 1**. If the white paper is approved, the vendor receives an "Invitation to Submit" a full technical and cost proposal (**Step 2**).
- **Commercial Solutions Openings (CSOs) & Other Transaction Authorities (OTAs):** When the military looks to procure fast-tracked, commercial dual-use innovations, it relies heavily on short white papers (usually 3–5 pages) rather than traditional, restrictive federal contracts.
- **Pre-Eligibility for SBIR / STTR Open Topics:** Many innovative "Open Topics" within the DoD SBIR/STTR programs require an initial technical white paper to prove feasibility before advancing to Phase I or Phase II funding.

Suggested Scenarios (Proactive Pitches)

- **Responding to Requests for Information (RFIs):** When a command commands a market research survey (via platforms like SAM.gov), submitting an unsolicited or highly tailored white paper influences how the military eventually shapes its official requirements.
- **Internal Military Innovations:** Known as "**Catalyst Papers**" or "Information Papers" at the unit level, officers or enlisted personnel draft these to pitch a tactical change, a localized tech integration, or a solution to a commanding officer.

2. How They Are Used

Once a white paper enters the system, it serves as an internal strategic mechanism:

- **Triage Tool:** Commands use them to quickly filter out vendors who do not understand the military environment or whose tech is not mature enough.
- **Down-Selection Mechanism:** It transitions an open pool of hundreds of interested applicants into a hand-selected group of 5–10 entities invited to pitch live or submit full RFPs.
- **Requirements Shaping:** If a white paper presents a compelling capability that leadership didn't know existed, they will use its parameters to write the requirements for a future program of record.

3. How They Are Evaluated

Military reviewers evaluate white papers based on a standardized framework, often referred to as the **Heilmeier Catechism** or formal BAA criteria. Evaluators score submissions using three primary lenses:

Evaluation Dimension	What Reviewers Look For
Technical Merit & Feasibility	Is the science sound? Reviewers verify your reported **Technology Readiness Level (TRL)**. They check if the solution works in denied, degraded, intermittent, or limited (**DDIL**) bandwidth environments, as flawless commercial internet cannot be expected at the tactical edge.
Defense Relevancy & Impact	Does this solve an explicit, documented warfighter capability gap? If it is "cool technology" without a clear, definitive concept of employment, it will be rejected.
Interoperability & Posture	Can this easily integrate into current command and control networks (like **JADC2**)? Does the vendor understand the security hurdles required to obtain an **Authority to Operate (ATO)** on military networks?
Rough Order of Magnitude (ROM)	Even if a detailed budget isn't required, reviewers check the **ROM price** page. If the solution is technically brilliant but costs more than the target command's entire annual innovation budget, it is dead on arrival.

*Note: Strict page limits (typically **3 to 10 pages**) are rigidly enforced. If a solicitation specifies a 5-page maximum, reviewers are legally mandated to stop reading at page 5 and discard the rest.*

Essential Tips for Innovation Pitches

- **Kill the Hype Words:** Avoid generic phrases like *"revolutionary next-generation paradigm shift."* Use metrics instead: *"Reduces data processing latency from 45 minutes to 12 seconds."*
- **Emphasize DDIL (**Denied, Degraded, Intermittent, and Limited**):** If your technology requires a flawless, constant 5G internet connection to work, the military cannot use it at the tactical edge. Explicitly detail how your innovation behaves when networks are jammed or disconnected.
- **Address the ATO Early:** Acknowledge security frameworks. Demonstrating that you understand the **Authority to Operate (ATO)** process establishes immediate credibility with military IT and acquisition officers.

To help optimize the below template for your specific project, you will need to know:

- What **Technology Readiness Level (TRL)** is your innovation currently at?
- Is this a **software-only** solution, a **hardware** system, or a mix of both?
- What specific **military branch, agency, or innovation hub** (e.g., DIU, AFWERX, Army Applications Lab) are you pitching to?

White Paper Template

CLASSIFICATION: [UNCLASSIFIED // CUI // SECRET]

CONTROL NUMBER: [Insert Number]

INNOVATION WHITE PAPER NAME

PROJECT CODENAME / SYSTEM NAME: [e.g., Project AETHER / Autonomous Heavy Transport]

TECHNOLOGY DOMAIN: [e.g., Cyber, AI/ML, Unmanned Systems, Directed Energy]

DATE: [DD Month YYYY]

ORIGINATING AGENCY/ENTITY: [Commercial entity, Defense Lab, or Unit Innovation Cell]

PREPARED BY: [Name, Title, Organization/Rank]

TECHNICAL POC: [Name, Contact Info for Lead Engineer/Scientist]

MILITARY SPONSOR (If applicable): [Rank/Name, Unit, Duty Position]

1. PURPOSE & VALUE PROPOSITION

Provide a 2–3 sentence overview of the innovation. Explicitly state what commercial or novel technology you are adapting and the high-level value it brings to the warfighter (e.g., "Reduces logistics footprint by 30%," "Automates threat identification at the tactical edge").

2. EXECUTIVE SUMMARY

Bottom Line Up Front (Bluff): The Innovation Impact

Deliver a 200-word executive summary for non-technical senior leaders.

* What is the innovation?

* What critical military bottleneck or capability gap does it break?

* What is the immediate "ask" or next step? (e.g., Funding for Phase II SBIR, a 30-day field trial, or integration into an upcoming Joint Exercise).

3. PROBLEM STATEMENT & WARFIGHTER BOTTLENECK

Describe the existing operational problem or technological limitation using current military paradigms.

* Current Vulnerability: What can the adversary currently exploit, or what system is failing due to legacy technology?

* Warfighter Burden: How does the status quo negatively affect cognitive load, response time, or logistical chains?

* Operational Risk: What is the cost of letting this innovation gap go unaddressed?

4. THE INNOVATION SOLUTION & TECHNICAL OVERVIEW

Explain the technology simply but with engineering rigor. Use universal terms rather than proprietary corporate jargon.

* How It Works: Detail the core architecture, software framework, or hardware capabilities.

* TRL/MRL Status: State the current Technology Readiness Level (TRL) and Manufacturing Readiness Level (MRL) (e.g., TRL 4: Component validation in lab vs. TRL 7: Operational environment prototype).

* Unique Defense Advantage: What makes this solution significantly faster, cheaper, or more lethal than current defense alternatives?

5. MILITARY INTEGRATION & INTEROPERABILITY

Military leaders will not adopt technology that creates an isolated silo. Detail how this innovation plugs into the existing ecosystem.

* System Interoperability: How does this interact with current Command and Control (C2) systems or Joint All-Domain Command and Control (JADC2) frameworks?

* Hardware/Software Footprint: Does it require heavy hardware modification or can it run via a simple software patch/containerized application?

* Cyber & Security Posture: State your path toward an Authority to Operate (ATO). Is the software containerized? Is it compliant with Zero Trust Architecture? Does it operate in denied, degraded, intermittent, or limited (DDIL) bandwidth environments?

6. FIELDING, LOGISTICS, & SCALABILITY PATH

Explain how the military can scale this from a lab prototype to a deployed asset.

* Training & Human Factors: How much specialized training does a warfighter need to operate this? (e.g., "Requires less than 2 hours of train-the-trainer instruction").

* Supply Chain & Sustainment: Are critical components sourced from foreign adversaries? Can it be maintained at the organic (unit) level or does it require contractor-managed logistics?

7. PROPOSED TRANSITION PLAN & COURSE OF ACTION (COA)

Outline a pragmatic roadmap for testing and procurement.

* Phase 1 (Immediate - Next 60 days): Lab demonstration or software integration testing.

* Phase 2 (Mid-term - 6 months): Limited operational utility assessment during a military exercise (e.g., Project Convergence, Northern Edge).

* Phase 3 (Long-term - 12+ months): Procurement path (e.g., transitioning via OTAs, Middle Tier of Acquisition, or SBIR Phase III).

8. RESOURCE REQUIREMENT & THE "ASK"

Be explicit about what resources are needed to take the next step.

* Financial Footprint: Estimated cost for a prototype build, pilot program, or full deployment.

* Military Support Needed: Request for specific military data sets, access to a range/testbed, or dedicated personnel for user-feedback loops.

APPENDIX: TECHNICAL VALIDATION & DATA

[Attach peer-reviewed studies, lab testing data, cyber penetration results, or letters of support from existing military field testers.]