GENERAL Q&A FOR FUTURE OFFERORS
SBIR TOPIC AF254-D0802: AI/ML - ENHANCED RISK MANAGEMENT FRAMEWORK

Which parts of the RMF process are we expected to automate? Must it be "all of RMF"?

Phase II must demonstrate a TRL-6 prototype that automates the RMF elements you already proved feasible in your Phase I-type work. Example areas include control tailoring, evidence ingestion/normalization, POA&M generation, and continuous-monitoring dashboards. Full end-to-end automation is not required in Phase II; prioritize the pieces that shorten the path to an ATO and feed directly into Phase III's cATO + ConMon objective.

Traditional ATO, cATO, or both?

Design should not preclude future cATO workflows; however, Phase II evaluation will use a standard ATO package.

Are any RMF tasks "off-limits" to automation?

Tasks that require inherently governmental judgment—risk acceptance by the Authorizing Official and final SCA concurrence—must keep a human-in-the-loop. Everything else is fair game if you can show outcome quality at least equal to the current manual baseline.

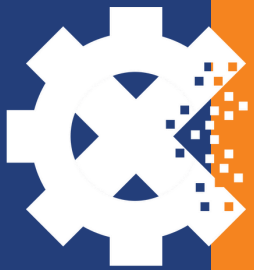Which DoD systems/APIs are priority for integration?

The government is coordinating to provide an eMASS sandbox (IL4/5) to offerors who wish to test their product. High-value feeds identified by stakeholders are ACAS/Tenable, STIG automation output, HBSS/ESS, and Nessus Agent results. Use open, machine-readable formats (JSON, OSCAL, YAML) wherever possible.

Deployment environment—Cloud One, Platform One, on-prem? IL levels?

Recommended practice: target IL4/5 first; design so it can be re-hosted at IL6 or higher on demand. A FedRAMP-High (IL4/5) cloud such as Cloud One Azure is acceptable for Phase II as long as you can export data required for eventual on-prem installs at classified levels.

Are specific AI/ML stacks required or prohibited?

No mandated stack. Your technical volume must justify model choice, training-data provenance, and how you will meet DoD Responsible-AI guardrails. Black-box SaaS models that cannot be audited are discouraged.

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-D0802: AI/ML - ENHANCED RISK MANAGEMENT FRAMEWORK

Primary user persona—RMF engineers only?

Design recommendation: Phase II UI/UX should serve RMF practitioners first (ISSM, SCA, AO staff) but expose read-only dashboards that non-cyber decision-makers can consume without training.

Will sample artefacts or realistic traffic be provided?

Offerors should plan to obtain representative artefacts; Government may provide sample data subject to classification and CUI constraints. Synthetic network traffic is acceptable for Phase II development; live feeds come later.

What volume of data should we expect?

Estimate based on stakeholder discussions: roughly 8-10 GB per system per assessment cycle (documents, screenshots, scan CSVs).

What metrics will justify future funding or adoption?

Follow-on funding or Phase III opportunities have not been announced. Suggested metrics include:
• Percent reduction in calendar days to ATO decision
 • Labor hours saved per control family
 • Evidence re-use rate across systems
 • False-positive versus true-positive control-failure detection

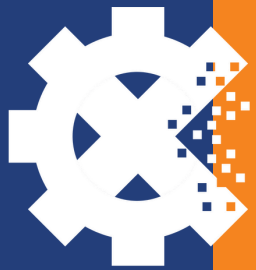Single monolithic solution or multiple micro-apps?

Either is acceptable; evaluation criteria weight a coherent end-to-end workflow and ease of integration higher than packaging. Make your architectural choice explicit in the proposal.

Do we need to name the candidate system that already has an ATO?

No. The Government will furnish a representative test bed and sanitized data set; offerors do not need to name or secure access to an existing ATO'd system for Phase II.

How many Phase II awards will be made?

One (1).

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-D0802: AI/ML - ENHANCED RISK MANAGEMENT FRAMEWORK

Timeline:

Next AMA: May 22nd
Applications Open:
May 28th
Applications Close:
June 25th

To Apply:

https://afwerx.com
/divisions/ventures
/specific-topic/

Questions or to discuss more:

sbir.sttr@afcyberworx.
org

What travel should we budget for Phase II?

Required travel is not anticipated. Reviews and demonstrations are expected to be conducted virtually; in-person visits will be arranged only if mission-essential and approved by the Government.

How do we show Phase I feasibility in a Direct-to-Phase II (D2P2) proposal?

Show Phase I feasibility by placing, in Volume 5 of the D2P2 package, a short synopsis plus the detailed "feasibility documentation" (no page limit) that proves you already achieved the topic's Phase I goals: lab or pilot results for a TRL 4-6 prototype, test reports, demo video or screenshots, and a table that cross-walks each Phase I requirement to the exact evidence page. The Air Force will not even evaluate a D2P2 if this file set fails to establish scientific and technical merit, or if the work was done under any prior SBIR/STTR; it must have been "substantially performed" by your firm/PI and you must own or license any associated IP.

Is CUI processing required during Phase II?

Not during the prototype, but your architecture must be upgradable to Moderate-level CUI. Use FIPS-validated cryptography and document how you will inherit CMMC Level 2 controls.

Are memory-safe languages or supply-chain frameworks desired?

This is not a mandatory requirement. Show how your technology choice mitigates common weakness categories.

What timeline milestones are expected?

Offerors should propose a milestone schedule that credibly achieves TRL 6 within the 24-month PoP.

Is there an integration-test API or export format we must use for RMF data?

The government is coordinating to provide an eMASS sandbox for testing. For initial proposals, no specific format is required.

Who owns the Phase III transition?

Initial stakeholder discussions are with SAF/CN (USAF CIO) and 16 AF's Enterprise Cyberspace & Information Dominance directorate. No Phase III owner has been identified.