AIR FORCE
CYBERWORX™

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

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

What is the end goal of this effort - operational deployment or experimental use?

The ultimate objective is operational deployment. While Phase I centers on feasibility, the desired outcome is a deployable system that functions within active defensive cyber operations. The decoy network should lure adversaries away from operational systems into high-fidelity, dynamic environments. These environments must also support persistent monitoring to gather actionable intelligence on adversary behavior and tactics. Solutions should be designed with real-world scalability, integration potential, and mission relevance in mind.

What level of realism and adaptability is expected in the decoy environment?

Realism is critical. The decoy must continuously evolve to remain believable under scrutiny from state-sponsored adversaries. This includes realistic user behavior, data flows, services, and infrastructure. The environment should appear valuable and exploitable—enticing enough to capture attention—but not so vulnerable or static that it is easily identified as a trap. AI/ML should be leveraged to monitor real or simulated networks and adapt the decoy in real time or through retraining. A well-calibrated balance of authenticity and stealth is essential for long-term deception.

What role should AI/ML play in the proposed solution?

AI/ML is expected to be central to the system's design. It should be used to learn from live, synthetic, or simulated network data—capturing behaviors, services, and traffic patterns—and generating decoy environments that mirror those observations. Additionally, AI/ML should drive adaptation over time, model user and adversary interactions, and detect intrusions or behavioral shifts. The solution should support autonomous updates and behavior generation while providing defenders with real-time insights into threat activity.

AIR FORCE CYBERWORX™

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

What operational modes and response capabilities should the system support?

The system must support fully autonomous, semi-automated, and manual control modes. Autonomous operation ensures persistent deception with minimal operator overhead. Semi-automated and manual controls enable tailored intervention during targeted threat tracking. The system should be capable of real-time response to adversary behavior—modifying topology, adjusting services, or escalating alerts as needed. This responsiveness increases the credibility of the decoy while enhancing operator situational awareness.

Are specific architectures, technologies, or protocols required?

No specific architecture is mandated. Offerors may use AI/ML, expert systems, virtualization, containerization, or hybrid approaches. The key requirement is a flexible, scalable system that can emulate real operational environments across a range of protocols (e.g., HTTP, MQTT, MODBUS, DNP3) and behaviors. The architecture should allow for realistic traffic and service emulation, seamless integration of learning pipelines, and continuous refinement based on observed inputs.

What deployment environments and integration considerations should be anticipated?

The system should be designed for deployment in a range of environments, including secure cloud, on-premises, or hybrid configurations. A FedRAMP-approved cloud is not required, but cybersecurity best practices and modular design are essential. Solutions should be aligned with long-term integration pathways, including Risk Management Framework (RMF) compliance and Authority to Operate (ATO) readiness. Flexibility, portability, and ease of deployment will be critical for successful transition to operational environments.

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

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

How is realism currently evaluated in decoy networks, and what heuristics matter most?

The key indicator is whether the adversary realizes they're in a decoy. If a hacker disengages early or alters their tactics, that's a sign the deception failed. Past efforts often lacked credible user behavior, protocol fidelity, or exhibited static responses—making them too easy to spot.

Should adaptability be aligned with known adversary TTPs (e.g., MITRE ATT&CK), or should it operate autonomously?

Either approach can be effective, but proposals should clearly define their strategy. Aligning with adversary TTPs offers transparency and control, while autonomous adaptation can offer broader flexibility. Systems that can learn, evolve, and reconfigure to remain convincing are the goal.

Will Phase II testing require specific sandbox environments?

No specific testbed is currently designated. Phase I proposers should suggest an appropriate sandbox or simulation plan for future evaluation, showing how their architecture supports realism, adversary engagement, and dynamic behavior without needing a fixed environment.

What matters more—user behavior simulation or infrastructure fidelity?

Both are important, but adversaries often detect fakes through inconsistencies in user behavior and data flow patterns. A convincing rhythm of interaction—user logins, file access, network chatter—can outweigh perfect system specs.

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.stttr@afcyberworx.org

AIR FORCE CYBERWORX™

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

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

Should decoy systems aim for adversary characterization, or is tracking enough?

Detection and tracking are baseline. If done securely, extracting insights about adversary behavior, tools, or intent adds significant value. However, attribution is secondary to effective deception and must not risk exposure of the decoy.

Will these decoy systems integrate into broader SOC or DCO toolchains?

Yes, that's the anticipated direction. Interoperability with other cybersecurity platforms will enhance value, especially if systems support standards like STIX/TAXII or OpenC2 for alert sharing and orchestration.

What types of networks might decoys be expected to emulate?

Proposers should be prepared to replicate a range of environments—enterprise IT, industrial control systems (ICS/SCADA), telecom infrastructure, or operational DoD networks. Modularity and mission-specific tailoring will be advantageous.

Are there any SWaP or software restrictions, and should decoys support edge deployment?

Centralized deployment is generally preferred, but edge-capable systems are viable, especially in contested environments. If edge-launch is envisioned, the Phase I feasibility study should clearly articulate how bandwidth, SWaP, and security concerns will be addressed.

AIR FORCE
CYBERWORX™

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

GENERAL Q&A FOR FUTURE OFFERORS

SBIR TOPIC AF254-0801: AI/ML - GENERATED DECOY NETWORKS

What are the gaps in existing commercial decoy solutions?

Many commercial products lack the depth, adaptability, or automation needed to deceive advanced actors. They're often static, manually configured, or easily fingerprinted. This topic seeks solutions that feel alive to an adversary—adaptive, dynamic, and difficult to dismiss.

What is the cost structure for a Phase I award?

Phase I proposals may request up to $140,000 for a 6-month effort. Emphasis should be placed on feasibility, automation potential, and operational relevance —especially in contested environments.

What documentation is required for proposal submission?

Submissions include seven volumes: Cover Sheet, Technical Volume, Cost Volume, Company Commercialization Report, Supporting Documents, Fraud, Waste & Abuse acknowledgment, and Foreign Disclosures. See the official DAF STTR Phase I instructions (Release 8) and the DSIP portal for full details.

Will data be provided to support training or validation?

No government datasets will be furnished in Phase I. Proposers should rely on public or synthetic data. If access to sensitive or representative data is essential for advancement, that need should be described in the feasibility study with a plan for how it would be addressed.