Defense Threat Reduction Agency (DTRA)
2027 Small Business Technology Transfer (STTR) BAA
Release 2
Proposal Submission Instructions

INTRODUCTION

The Defense Threat Reduction Agency (DTRA) mission is to enable the Department of War (DoW), the U.S. Government, and International Partners to counter and deter Weapons of Mass Destruction (WMD) Chemical Biological, Radiological, Nuclear and Improvised Threat Networks. The DTRA SBIR program is consistent with the purpose of the Federal SBIR/STTR Program, i.e., to stimulate a partnership of ideas and technologies between innovative small business concerns and through Federal-funded research or research and development (R/R&D).

The approved 2027 topics solicited for the Defense Threat Reduction Agency (DTRA) Small Business Innovation Research (SBIR) Program are included in these instructions followed by the full topic description. Offerors responding to this Broad Agency Announcement (BAA)solicitation must follow all general instructions provided in the related Department of War Annual Program BAA and submit proposals by the date and time listed in this release. Specific DTRA requirements that add to or deviate from the DoW Annual Program BAA instructions are provided below with references to the appropriate section of the DoW document.

Proposers are encouraged to thoroughly review the DoW Annual Program BAA and register for the DSIP Listserv to remain appraised of important programmatic and contractual changes.

- The full DoW solicitation is available on DSIP at https://www.dodsbirsttr.mil/submissions/solicitation-documents/active-solicitations. Be sure to select the tab for the appropriate solicitation cycle.
- Register for the DSIP Listserv at: https://www.dodsbirsttr.mil/submissions/login.

Specific questions pertaining to the administration of the DTRA SBIR/STTR Program and these proposal preparation instructions should be directed to:

Ms. LaTracia Price
DTRA SBIR/STTR Program Manager
LaTracia.T.Price.civ@mail.mil
Tel: 571-616-6583

Defense Threat Reduction Agency
8725 John J. Kingman Road
Stop 6201
Ft. Belvoir, VA 22060-6201

PHASE I PROPOSAL GUIDELINES

The DoW SBIR/STTR Innovation Portal (DSIP) is the official portal for DoW SBIR/STTR proposal submission. Proposers are required to submit proposals via DSIP; proposals submitted by any other means will be disregarded. Detailed instructions regarding registration and proposal submission via DSIP are provided in the DoW solicitation.

Proposal Coversheet (Volume 1)
The proposal coversheet is prepared on DSIP and in accordance with the DoW solicitation.

Technical Volume (Volume 2)
The technical volume is not to exceed 20 pages and must follow the formatting requirements provided in the DoW. Pages within the 20th page range will be considered in proposal evaluations.

Content of the Technical Volume

A Phase I Proposal Template is available to provide helpful guidelines for completing each section of your Phase I technical proposal. This can be found at Training Materials (dodsbirsttr.mil)

Offerors should follow the DoW SBIR Program BAA guidelines regarding Technical Volume content.

Cost Volume (Volume 3)

The Phase I Base amount, not including the amount allocated for TECHNICAL AND BUSINESS ASSISTANCE (TABA), must not exceed $250,000.00. All costs must be clearly identified on the Proposal Cover Sheet (Volume 1) and in Volume 3. DTRA requires the use of the attached excel spreadsheet for the Cost Volume. The cost template becomes visible to the offeror when the Cost Volume is initiated.

The DTRA Cost Volume template 2027 will be accessible once the Cost Volume is initiated.

IMPORTANT: When completing the cost volume, you must provide enough information to allow the agency to understand how you plan to use the requested funds if a contract is awarded. Itemized costs of any subcontract or consultant should be provided to the same level as for the prime small business. If an unsanitized version of costs cannot be provided with the proposal, the Government may request it during negotiations if selected. Refer to the instruction provided in the DoW Annual SBIR program BAA for additional details on the content of the Cost Volume.

Note 1: Cost for travel funds must be justified and related to the needs of the project.
Note 2: Attachment – DTRA SBIR/SITTR Program Funding Limits

Please review the updated Percentage of Work (POW) calculation details included in the DoW Program BAA.

For SBIR projects, DTRA normally will not accept any deviation to the POW requirements, however if discovered during review in Contracting, the offeror may be allowed to revise the cost proposal to be in line with the POW requirements.

Note: SBIR projects, DTRA normally will not accept any deviation to the POW requirements, however if discovered during review in Contracting, the offeror may be allowed to revise the cost proposal to be in line with **DTRA's requirement limits.**

Page Limit, Cost and Duration:

Project Phase	Technical Vol Page Limit	Cost	Duration
Phase I	20 pages	$250,000.00	7 Months

Company Commercialization Report (CCR) (Volume 4)

Completion of the CCR as Volume 4 of the proposal submission in DSIP is required. Please refer to the DoW SBIR Program BAA DoW solicitation for full details on this requirement. Information contained in the CCR will not be considered by DTRA during proposal evaluations.

Supporting Documents (Volume 5)

Volume 5 is provided for proposing SBCs to submit additional documentation to support the Coversheet (Volume 1), Technical Volume (Volume 2), and the Cost Volume 3). Please refer to the DoW solicitation for more information.

All proposing small business concerns are mandatory to submit the following documents to Volume 5:

Note: Contractor Certification Regarding Provision of Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment.
Note: Offerors having any concerns pertaining to mandatory requirement as stated above should provide a mitigation plan addressing the concerns.

Fraud, Waste and Abuse Training (Volume 6)
Fraud, Waste and Abuse training material can be found in the Volume 6 section of the proposal submission module in DSIP and must be thoroughly reviewed once per year to proceed with proposal submission.

Disclosures of Foreign Affiliations or Relationships to Foreign Countries (Volume 7)
Small business concerns must complete the Disclosures of Foreign Affiliations or Relationships to Foreign Countries webform in Volume 7 of the DSIP proposal submission. Please be aware that the Disclosures of Foreign Affiliations or Relationships to Foreign Countries WILL NOT be accepted as a PDF Supporting Document in Volume 5 of the DSIP proposal submission. Do not upload any previous versions of this form to Volume 5. For additional details, please refer to the DoW Program BAA.

PHASE II PROPOSAL GUIDELINES

Phase II proposals may only be submitted by Phase I awardees.
Those small business concerns submitting a Phase II proposal should plan to submit a fully developed proposal into the DSIP proposal system within thirty (30) days after the end of the Phase I period of performance. The small business concern may or may not be notified of the proposal's due date.

The Phase II proposal's Technical Volume should not exceed 20 pages and should generally follow the outline and structure of Phase I to include benefits or lessons learned from the Phase I effort.

DTRA's has decided that all Phase II project are not to exceed (NTE) 24-month duration, and a ceiling price of $1,500,000

DISCRETIONARY TECHNICAL AND BUSINESS ASSISTANCE (TABA)

In accordance with of the Small Business Act (15 U.S.C. § 638(q)) and the Small Business Innovation and Economic Security Act of 2026 (P.L. 119-83), the Defense Threat Reduction Agency (DTRA) authorizes recipients of Phase I and Phase II awards to request TABA funding to use for eligible services.

These business-related services are designed to improve the commercialization success of small business concerns. This includes providing access to a network of scientists and engineers across a wide range of technologies or providing access to technical and business databases

Allowed TABA Focus Areas

- Technical Decision Making
    - Making improved, evidence-based technical decisions concerning the project.
- Technical Problem Solving
    - Addressing and solving technical challenges that arise during project execution.
- Risk Mitigation
    - Minimizing overall technical risks associated with the project.
- Product Commercialization
    - Developing and commercializing new products or processes resulting from the project.
- Cybersecurity Compliance
    - Assistance with meeting federal and agency cybersecurity requirements.

If you are proposing use of Discretionary Technical and Business Assistance (TABA), you must provide a cost breakdown in the Cost Volume under "Other Direct Costs (ODCs)" and provide a one-page description of the vendor you will use and the Technical and Business Assistance you will receive. For the Phase I project, the amount for TABA may not exceed $6,500 per award. For the Phase II project, the TABA amount may be less than, equal to, but not more than $50,000 per project. The description should be included in Volume 5 of the proposal. TABA activity costs are line item portioned into the contract price.
Approval of Discretionary Technical and Business Assistance is not guaranteed and is subject to review of the contracting officer.

For Discretionary Technical and Business Assistance, small business concerns may propose one or more vendors. Additionally, business-related services aimed at improving the commercialization success of a small business concern may be obtained from an entity, such as a public or private organization or an agency or other entity established or funded by a State that facilitates or accelerates the commercialization of technologies or assists in the creation and growth of private enterprises that are commercializing technology.

TECHNICAL EVALUATION AND SELECTION

All proposals will be evaluated in accordance with the evaluation criteria listed in the DoW SBIR Program BAA. DoW solicitation.

Proposing firms will be notified of selection or non-selection status for a Phase I award within 90 days of the closing date of the BAA. DTRA has a single Evaluation Authority (EA) for all proposals received under this solicitation. The EA either selects or rejects Phase I and Phase II proposals based upon the results of the review and evaluation process plus other considerations including limitation of funds, and investment balance across all the DTRA topics in the solicitation. To provide this balance, a lower rated proposal in one topic could be selected over a higher rated proposal in a different topic. DTRA reserves the right to select all, some, or none of the proposals in a particular topic.

Notifications

Following the EA decision, the DTRA SBIR/STTR office will release notification e-mails of selection or non-selection status for a Phase I award within 90 days of the closing date of the BAA. The E-mails will be sent to the addresses provided for the Principal Investigator topic and listed Corporate Official.

Offerors may request a debriefing of the evaluation of their not selected proposal and should submit this request via email to: dtra.belvoir.RD.mbx.sbir@mail.mil; the subject line must include **"SBIR or STTR Program the full BAA Proposal number T27TZ-NV00X-0XXX - Debriefing Request."** Debriefings are provided to help improve the offeror's potential response to future solicitations. Debriefings do not represent an opportunity to revise or rebut the EA decision.

For selected offers, DTRA Topic Author will build an acquisition package for Finance and the Contract Officer (KO) approval to move to contract execution which is subject to Procurement Acquisition Timeline (PALT) of 120-days to execute the award. DTRA Phase I awards are issued as fixed-price purchase orders with a maximum period of performance of seven months. DTRA may complete Phase I awards **without additional negotiations** by the contracting officer or without opportunity for revision for proposals that are reasonable and complete.

DTRA Support Contractors

Select DTRA-employed support contractors may have access to contractor information, technical data or computer software that may be marked as proprietary or otherwise marked with restrictive legends. Each DTRA support contractor performs under a contract that contains organizational conflict of interest provisions and/or includes contractual requirements for nondisclosure of proprietary contractor information or data/software marked with restrictive legends. These contractors require access while providing DTRA support such as advisory and assistance services, contract specialist support, and support of the Defense Threat Reduction Information Analysis Center (DTRIAC). The contractor, by submitting a proposal or entering into this contract, is deemed to have consented to the disclosure of its information to DTRA's support contractors.

Offerors are advised that employees of commercial firms under contract to the Government may be utilized to provide administrative, technical, or advisory support during the proposal evaluation process and subsequent contract administration.

These support contractors may require access to proposals, including proprietary and confidential information, solely for the purpose of providing this required support to the Government. Support contractors are strictly prohibited from evaluating proposals or making any source selection decisions.

To protect offeror information, the Government ensures that all such support contractors are bound by strict corporate and individual Non-Disclosure Agreements (NDAs). These NDAs legally prohibit the unauthorized disclosure of offeror proprietary, confidential, and source selection sensitive information. Furthermore, these support contractors are subject to rigorous Organizational Conflict of Interest (OCI) clauses that restrict them from using the information for any competitive advantage or for any purpose other than providing the contracted support to DTRA.

By submitting a proposal, the offeror acknowledges that their proposal information may be disclosed to these authorized support contractors for the limited support purposes stated above. Offerors remain responsible for ensuring that all proprietary information within their proposal is appropriately marked in accordance with the solicitation instructions.

Protests

Refer to the DoW SBIR Program BAA for procedures to protest the Announcement.

As further prescribed in FAR 33.107(b), FAR 52.233-3, Protests after Award should be submitted in accordance with FAR Subpart 33.1 – Protests.

Protests filed with the Government Accountability Office (GAO) must be served on the cognizant Contracting Officer identified in the specific topic instructions or associated award document. A courtesy copy of such protests should also be provided to the SBIR STTR Program Manager, LaTracia Price. (addressed to Don Shires as follows) by obtaining written and dated acknowledgment of receipt from (if mailed letter) Defense Threat Reduction Agency, ATTN: J4CR, Don Shires, 8725 John J Kingman Road, Fort Belvoir, VA 22060-6201. If Federal Express is used for the transmittal, the appropriate address is Defense Threat Reduction Agency, ATTN: J4CR, Don Shires8725 John J Kingman Road, Fort Belvoir, VA 22060-6201.

AWARD AND CONTRACT INFORMATION

On average, DTRA received 350 proposals per topic cycle and awards up to 17 - 20 or .06 percent of the received proposals under a topic cycle. For fiscal year 2027, DTRA plans to utilize its Department of War (DoW) SBIR STTR Program budget proportioned to award a number of firm-fixed-price (FFP) Phase I projects by way of Purchase Order each PO value not to exceed $250,000.00 for a (7) month period of performance with the six months devoted to the research and the final month for the final report. Notwithstanding TABA maximum of $6,500.00 for the entire project. Additionally, DTRA plans to use the balance of the budgets portion to award follow-on Phase II project, using a definitive cost (COST) contract for each award not to exceed $1,500,000 for a duration not to exceed 24-month period of performance. Notwithstanding TABA maximum $50,000.00 between the combined phase II projects.

ADDITIONAL INFORMATION

The International Traffic in Arms Regulations (ITAR), 22 CFR Parts 120 through 130, and the Export Administration Regulations (EAR), 15 CFR Parts 730 through 799, will apply to all projects with military or dual-use applications that develop beyond fundamental research, which is basic and applied

research ordinarily published and shared broadly within the scientific community. More information is available at https://www.pmddtc.state.gov/ddtc_public.

The technology within some DTRA topics is restricted under export control regulations including the International Traffic in Arms Regulations (ITAR) and the Export Administration Regulations (EAR). ITAR controls the export and imports of listed defense-related material, technical data and services that provide the United States with a critical military advantage. EAR controls military, dual-use and commercial items not listed on the United States Munitions List or any other export control lists. EAR regulates export-controlled items based on user, country, and purpose. **The offeror must ensure that their firm complies with all applicable export control regulations.**

NOTE: Export control compliance statements found in these proposal instructions are not meant to be all inclusive. They do not remove any liability from the submitter to comply with applicable ITAR or EAR export control restrictions or from informing the Government of any potential export restriction such as fundamental research and development efforts proceed.

DTRA
SBIR DOW 2027 BAA
Topic Index
Release 2

DTR27TZ02-NV001	Biolab Mirror: Artificial Intelligence / Machine Learning (AI/ML) Digital Twin for Intent Characterization and Bio-Containment Integrity
DTR27TZ02-NV002	AI/ML Verification of Microelectronic Integrity for High-Assurance Systems
DTR27TZ02-NV003	Compact High Energy Density Capacitors For Pulsed Field X-Ray Generators

DTR27TZ02-NV001 TITLE: Biolab Mirror: Artificial Intelligence / Machine Learning (AI/ML) Digital Twin for Intent Characterization and Bio-Containment Integrity

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Trusted AI and Autonomy

PROJECTED CMMC LEVEL REQUIREMENT: Level 1

OBJECTIVE: Develop a high-fidelity "Digital Twin" (The Biolab Mirror) and an advanced Artificial Intelligence / Machine Learning (AI/ML) methodology capable of continuous, non-invasive integrity verification and intent characterization of a mid-size, state-sponsored biological research facility. The solution must fuse continuous physical/biological signatures (e.g., metabolic output, environmental thermodynamics, material logistics) with discrete digital telemetry (e.g., Laboratory Information Management Systems (LIMS) logs, Supervisory Control and Data Acquisition (SCADA) / Building Management Systems (BMS) control data). The objective is to detect clandestine biological activities, containment spoofing, and the subtle operational drift indicative of a transition from peaceful, declared research to unauthorized, non-compliant, or undeclared high-risk biological material production [1][2].

This effort bridges a critical gap between standard Information Technology (IT) network defense and biological physical reality by establishing a “Zero Trust” posture that cross-validates digital telemetry against the immutable laws of physics. Unlike current commercial cyberbiosecurity offerings that focus solely on the IT perimeter or traditional biosurveillance platforms that are purely reactive, the Biolab Mirror is proactively designed to characterize nefarious intent before unauthorized, non-compliant, or undeclared high-risk biological material production occurs.

DESCRIPTION: The proliferation of dual-use biological technologies and automated, high-containment laboratories globally presents a profound challenge to arms control verification and biosurveillance [3]. A state-sponsored facility operating under a declared, peaceful mandate (e.g., vaccine development, agricultural research) possesses all the necessary infrastructure, reagents, and personnel to rapidly pivot to unauthorized, non-compliant, or undeclared high-risk biological material production [2]. Current verification methods rely heavily on periodic physical inspections, voluntary declarations, and audits of digital LIMS. However, advanced adversaries can digitally spoof BMS, manipulate LIMS records, and conceal clandestine pathogen scaling through “population ghosting” [4][5]. The Department of War (DoW) requires a “Physics-to-Mesh Zero Trust” architecture [6]. This solicitation seeks proposals for a “Biolab Mirror”—a comprehensive Digital Twin that does not inherently trust digital control logs. Instead, the Mirror must continuously cross-validate digital telemetry against the unalterable laws of physics, chemistry, and biology (Conservation of Mass, Thermodynamics, Metabolic Rates). By establishing a rigorous physical baseline (e.g., correlating total water inflow with Effluent Decontamination System (EDS) out-flow, or matching documented animal feed procurement to autoclave waste mass and vivarium Carbon Dioxide (CO_2) exhaust), the AI/ML engine must automatically flag the subtle “Coherence Failures” that betray clandestine pathogen scaling, undeclared animal models, or spoofed containment boundaries.

SUPPLEMENTAL INFORMATION

1. Programmatic Metrics and Data Sourcing

- Data Sourcing Strategy Synthetic Baseline Generation (Performer Sourced): The performer is responsible for generating the Phase II training and validation datasets using established biological and physical engineering standards.
- Phase I Exit Metrics Measure of Performance (MOP) 1 (Architecture Delivery): Deliver a Digital Twin architecture mapping cross-domain signatures including specialized cross-domain digital and physical validation points.

2. Strategic Offshoots & Cyber-Physical Emulation

- Executive Summary: The primary objective of the Biolab Mirror SBIR/STTR is defensive: to establish a high-fidelity "Physics-to-Mesh Zero Trust" baseline to detect clandestine activity and intent. Successful completion yields a secondary strategic asset: a perfect, un-spoofed "Cyber-Terrain" map that can be ported into isolated cyber-ranges to simulate, analyze, and train against multi-domain attacks targeting critical high-containment infrastructure [10].
- The Capability Gap in Current Cyber-Ranges: Current cyber-ranges are optimized for IT network emulation and struggle to accurately emulate OT and the physical realities of a BSL-3/BSL-4 environment.
- The Biolab Mirror as the Emulation Foundation: The Biolab Mirror solves this gap. By mapping the continuous physical signatures directly to the discrete digital telemetry, the performer constructs a fully functional Cyber-Physical Sandbox.
  The Attack Simulation: Authorized cybersecurity evaluation teams and system auditors can execute multi-stage simulated attacks against this virtual target (e.g., spear-phishing an academic researcher -> pivoting to the BMS network -> manipulating the Effluent Decontamination System). The Red Team must navigate the actual laws of biology and thermodynamics to succeed.
- Strategic ROI & Follow-On Potential: Authorizing the Biolab Mirror effort provides a "two-for-one" return on investment (ROI), yielding a defensive characterization engine and a foundational architecture for dedicated cybersecurity testing and critical infrastructure protection.

PHASE I:

- Architecture & Signature Mapping: Develop the conceptual architecture for the Biolab Mirror. The performer must comprehensively map all critical signatures of a mid-size Biosafety Level 3 (BSL-3) / Biosafety Level 4 (BSL-4) facility, categorizing them into Continuous (Physical/Biological) and Discrete (Digital/Telemetry) domains [7].
- Physics-to-Mesh Framework: Define the "Coherence Fuses" and mathematical models required to cross-validate specific digital assertions (e.g., BMS reporting "Sterilization Complete") with

physical ground truth (e.g., calculated facility equipment power utilization metrics or chemical reagent depletion).

- Intent Characterization Roadmap: Develop an AI/ML roadmap demonstrating how the Mirror will analyze deviations from the established facility baseline to detect the transition from legitimate research to unauthorized, non-compliant, or undeclared high-risk biological material production. This roadmap must include not only mass-balance analysis (detecting how much is being produced) but also Procurement Vector Analysis (detecting what is being produced).
- Resource Prioritization Strategy: Design a tiered sensor deployment strategy that maximizes the use of existing, zero-cost facility infrastructure while identifying the critical "Choke Points of Transduction" requiring specialized physical validation.
- Final Deliverable: A comprehensive Phase I report detailing the Digital Twin conceptual architecture, the mathematical coherence models, and a preliminary design for Phase II software implementation.

PHASE II:

- Prototype Development: Develop, demonstrate, and validate a working software prototype of the Biolab Mirror AI/ML engine.
- Synthetic Facility Ingestion: The prototype must successfully ingest and process a complex, simulated baseline dataset representing normal operations of a mid-size biological facility.
- Anomaly Detection: Utilize the prototype to successfully identify simulated "Coherence Failures" introduced into the dataset. Scenarios must include:
    - Population Ghosting: Detecting undocumented pathogen scaling or animal models via mass balance and metabolic discrepancies [9].
    - Containment Spoofing: Detecting unauthorized EDS discharges masked by manipulated operational technology telemetry [10].
    - Procurement Vector Validation: Demonstrate the prototype's capability to ingest, normalize, and categorize multi-source procurement registries.
- Transition Strategy: Provide a clear transition plan detailing how the Biolab Mirror architecture can be integrated into standard government biosurveillance architectures for remote facility assessment and biological risk verification [11].

PHASE III: DUAL USE APPLICATIONS:

- Government Application: Integration into standard government biosurveillance architectures for remote facility assessment and biological risk verification to quickly ascertain historical facility operations.

- Commercial Application: Transition to commercial pharmaceutical Quality Assurance / Quality Control (QA/QC), BSL-3/BSL-4 containment safety assurance, and insider-threat protection for proprietary genomic data and high-value biotechnology Intellectual Property (IP).

REFERENCES:

1. Department of Defense Directive (DoDD) 2060.02, Combating Weapons of Mass Destruction (CWMD) Policy, (2017).
2. National Academies of Sciences, Engineering, and Medicine (NASEM), Biodefense in the Age of Synthetic Biology, (2018).
3. World Health Organization (WHO), Global guidance framework for the responsible use of the life sciences: mitigating biorisks and governing dual-use research, (2022).
4. National Institute of Standards and Technology (NIST), Platform Firmware Resiliency Guidelines, Special Publication (SP) 800-193 (2018).
5. Peccoud, J., et al., "Cyberbiosecurity: From Naive Trust to Risk Awareness," Trends in Biotechnology, (2017).
6. Department of Defense Zero Trust Strategy, (November 2022).
7. Centers for Disease Control and Prevention (CDC) / National Institutes of Health (NIH), Biosafety in Microbiological and Biomedical Laboratories (BMBL), 6th Edition, (2020).
8. Environmental Protection Agency (EPA), Design Manual: Municipal Wastewater Stabilization Ponds, (1983).
9. American Association for Laboratory Animal Science (AALAS), Guide for the Care and Use of Laboratory Animals, 8th Edition, (2011).
10. Cybersecurity and Infrastructure Security Agency (CISA) Alert (AA20-205A), Recommend Immediate Actions to Reduce Exposure Across Operational Technology (OT) and Control Systems, (2020).
11. Defense Threat Reduction Agency (DTRA), Director's Strategic Intent 2025, (Fort Belvoir, VA: Office of the Director, February 3, 2025).

KEYWORDS: Digital Twin, Cyberbiosecurity, Intent Characterization, AI/ML, Bio-containment, Zero Trust, Biosurveillance

DTR27TZ02-NV002 TITLE: AI/ML Verification of Microelectronic Integrity for High Assurance Systems

OUSW (R&E) CRITICAL TECHNOLOGY AREA(S): Applied Artificial Intelligence (AAI)

COMPONENT TECHNOLOGY PRIORITY AREA(S): Trusted AI and Autonomy;#Microelectronics

PROJECTED CMMC LEVEL REQUIREMENT: Level 1

OBJECTIVE: Develop an innovative, Artificial Intelligence / Machine Learning (AI/ML) driven methodology and prototype architecture capable of non-destructively verifying the physical and logical integrity of Integrated Circuits (ICs). The solution must reliably detect sub-nanometer, adversarial Hardware Trojans that evade conventional functional testing. This ensures absolute trust in microelectronics utilized in high-assurance communications, critical infrastructure, and secure data collection systems, explicitly including protections against data-layer subversion and unauthorized RF activation. [1]

This effort bridges a critical gap between commercial supply chain illumination and physics-based national security hardware assurance. While current commercial offerings focus on firmware vulnerabilities and counterfeiting, they are blind to perfectly manufactured, sub-nanometer malicious logic such as Hardware Trojans. Furthermore, unlike existing programs such as DARPA AISS which operate in the pre-silicon design phase, this effort operates in the post-silicon verification phase assuming a "Zero Trust" posture.

DESCRIPTION: The Department of War relies heavily on advanced microelectronics sourced from a globally distributed commercial supply chain. Securing this supply chain against malicious insertion is a critical national security imperative, repeatedly highlighted by the Government Accountability Office (GAO) as a high-risk area. [2]

For defense systems operating in contested environments, compromised hardware represents a catastrophic vulnerability. Advanced adversaries are capable of introducing microscopic logic alterations (e.g., dopant-level Trojans, malicious dormant circuitry) during fabrication or transit. [3] A primary use case of concern involves hardware-level Trojans engineered to bypass software encryption, forcing ultra-secure communications gear or deployable sensor packages to execute unauthorized radio frequency (RF) transmissions, thereby exposing sensitive mission telemetry to hostile forces.

Furthermore, there is a critical emerging requirement to address sophisticated vulnerabilities residing between the hardware and firmware boundaries. The DoW seeks capabilities to identify malicious logic that facilitates unauthorized data inspection within the data layer, allowing an adversary to silently monitor, filter, or alter encrypted traffic streams at the silicon level. Additionally, the solution must investigate vectors where the data layer is manipulated to trigger unintended electromagnetic emanations from legitimate components, or the covert activation of dormant RF elements, for out-of-band exfiltration. [4]

The DoW seeks proposals for an automated, AI-driven inspection capability to mitigate these threats. The desired solution should ingest a Level 3 Technical Data Package (TDP) or Model-Based Systems

Engineering (MBSE) Digital Twin to establish a definitive baseline of intended logic gate behavior. It must then utilize advanced algorithms to process data from Non-Destructive Evaluation (NDE) techniques to physically and logically interrogate the delivered hardware against that baseline, identifying deviations that could enable data-layer subversion, unauthorized emissions, or system failure. [5]

Digital Provenance Integration: This effort seeks to establish an algorithmic layer of assurance compatible with modern secure supply chain initiatives. Proposals should consider the architectural requirements necessary for the proposed engine to interface with emergent DoW digital provenance frameworks, generating unique, verifiable identifiers for individual components before they are integrated into sensitive operational packages.

Data Sourcing Strategy

- Training Dataset (Performer Sourced): Performers must leverage synthetic data (MBSE/GAN generated) and existing open-source physical benchmarks to train models.
- Validation Dataset (Performer Sourced): The performer is responsible for the independent identification, procurement, and physical acquisition of the ICs and Digital Twins required for validation. This must be accomplished without assumption of reliance on Government Furnished Information (GFI); performers may propose use of appropriate GFI if such a database is known and available. This dataset must include a significant subset of components with specific, verified Hardware Trojans to ensure objective benchmarking.

FREQUENTLY ASKED QUESTIONS (FAQs)

FAQ 1.0: Commercial Market Overlap and Capability Gaps

- Q1.1: Several commercial companies utilize AI for quality assurance, and emerging platforms offer Deep Supply Chain Illumination and Firmware Assurance. How does this SBIR/STTR effort differ from these commercial offerings, and what specific gap does it close?
- A1.1: This SBIR/STTR bridges the gap between commercial supply chain illumination/firmware analysis and physics-based national security hardware assurance.
- Market Research Summary: The current commercial market includes advanced providers specializing in Deep Supply Chain Illumination, Hardware/Firmware Assurance, and Anti-Tamper & Forensics. Separately, major Failure Analysis (FA) labs utilize tools like Focused Ion Beam (FIB) and Scanning Electron Microscopy (SEM) for physical defect localization. [8]
- The Commercial Blind Spot: While firmware assurance platforms excel at identifying counterfeit parts and firmware-level vulnerabilities, they are generally blind to sub-nanometer, perfectly manufactured malicious logic etched directly into the silicon (Hardware Trojans). Furthermore, commercial AI inspection models are optimized for Yield and Reliability. A Hardware Trojan is not an error; it is a Deterministic Malicious Addition. Commercial models will pass a Trojaned chip because it meets all structural tolerances, blinding the supply chain to intentional sabotage. [9][10]
- Bridging the Gap: This proposal funds the development of Generative Adversarial Networks (GANs) that fuse these disciplines. It seeks to train detection algorithms to find intentionally hidden, malicious

logic that commercial defect scanners miss, anchoring that physical assurance to the secure supply chain.

FAQ 2.0: Programmatic Differentiation and Non-Duplication of Effort

- Q2.1: How does this proposed SBIR/STTR effort differ from the DARPA Automatic Implementation of Secure Silicon (AISS) program?
- A2.1: This proposal does not duplicate DARPA AISS. [7] AISS operates in the Pre-Silicon (Design) Phase, automating the insertion of security features into the IC blueprint. This SBIR/STTR operates in the Post-Silicon (Verification) Phase. It assumes a "Zero Trust" posture, acknowledging that adversaries may bypass AISS obfuscation during physical fabrication.

FAQ 3.0: Transition Strategy and the "Valley of Death"

- Q3.1: How does this Phase I/II proposal ensure a viable Phase III transition plan?
- A3.1: By structuring the output as a verification service capable of certifying COTS hardware, the technology becomes an enabling requirement for other acquisition programs. Primary transition targets include defense certification processes and rapid acquisition authorities.

FAQ 4.0: Data Rights and Intellectual Property (IP) Friction

- Q4.1: How will this initiative overcome the reluctance of commercial vendors to share proprietary Level 3 TDPs?
- A4.1: Performers are encouraged to design their AI/ML ingestion models using secure enclave or "zero-knowledge proof" principles to mathematically compare the physical scan against the Digital Twin without exposing human-readable schematics.

PHASE I: Conduct a feasibility study defining the proposed AI/ML architecture and the specific NDE data inputs required for high-fidelity anomaly detection.

Validation Dataset Strategy: Develop a comprehensive identification and procurement strategy for a high-fidelity validation dataset. This must detail how the performer will source, verify, and curate a diverse set of IC models and physical samples—including known "clean" and strategically "poisoned" variants—without assumption of reliance on Government Furnished Information (GFI); performer may propose use of appropriate GFI if such a database is known and available.

Develop a conceptual framework demonstrating the correlation of physical NDE scan data against a complex Digital Twin to identify logic-level alterations.

Data-Layer & RF Activation Vectors: Define preliminary investigation routes and algorithmic models specifically tailored to detect logic anomalies within the data layer, as well as vectors allowing data-layer manipulation for unintended EM emanations or discrete RF activation.

Model the system’s theoretical ability to detect distinct classes of Hardware Trojans (e.g., parametric, functional, dormant) without relying on "golden" physical reference chips.

Interoperability Hook: Identify and describe the architectural requirements for the proposed engine to interface with emergent DoW digital provenance and Supply Chain Risk Management (SCRM) frameworks. Specifically, identify how the AI/ML verification attestation can be cryptographically bound to the hardware's inherent Physical Unclonable Function (PUF), creating a unique identifier suitable for integration into a Distributed Ledger-based Chain of Custody. [6]

Metrics Alignment: Performers must explicitly demonstrate how their proposed research and conceptual architecture will meet or exceed the Threshold and Objective Measures of Performance (MOP) and Measures of Effectiveness (MOE) detailed in Enclosure 1: Programmatic Metrics and Data Sourcing.

Deliver a comprehensive Final Report detailing the algorithmic approach, computational requirements, and a preliminary design for a Phase II software/hardware prototype.

Phase I Exit Metrics

- MOP 1 (Architecture): Threshold: Deliver system architecture mapping NDE/TDP ingestion. Objective: Architecture includes a cryptographically secure "Zero-Knowledge" enclave design capable of identifying data-layer manipulation pathways.
- MOE 1 (Detection Capability): Threshold: Modeled AI demonstrates theoretical >85% detection of known functional Trojans in synthetic data. Objective: Theoretical >95% detection across multiple HT classes with simulated False Positive Rate (FPR) <5%.
- MOP 2 (Interoperability): Threshold: Define software API for cryptographic attestation output. Objective: Define methodology for securely binding the AI verification result to the hardware's PUF for DLT integration.
- MOP 4 (Data Strategy): Threshold: Complete a validated roadmap for acquiring physical and digital components for Phase II testing. Objective: Secured pre-commitments or established procurement channels for a diverse set of "poisoned" VLSI structures.

PHASE II: Develop, demonstrate, and validate a working prototype of the AI/ML verification engine. Procure and utilize the validation dataset identified in Phase I to benchmark the prototype’s detection accuracy, false-positive rate, and processing speed against the metrics outlined in Enclosure 1.

Demonstrate the algorithmic capability to adapt to novel insertion methods (e.g., adaptive learning) designed to subvert secure communications or trigger unauthorized emanations.

Adversarial Synthesis (GAN): Integrate a Generative Adversarial Network (GAN) architecture to autonomously synthesize "Compound Trigger" Hardware Trojans. The engine must demonstrate the ability to identify theoretical insertions that rely on the correlation of a legitimate operational state (e.g., high-readiness mode) with an anomalous external input vector.

Provide a clear transition plan detailing integration into existing DoW quality assurance pipelines, specifically interfacing with relevant DoW acquisition pathways and quality assurance centers.

Phase II Exit Metrics (Prototype Demonstration)

- MOE 2 (Physical Detection - "Performer-Procured Validation Set"): Threshold: Prototype processes the procured validation dataset with True Positive Rate (TPR) >90%. Objective: TPR >99%,

successfully identifying localized Hardware Trojans consisting of 10 or fewer manipulated logic gates within a VLSI structure.

- MOP 3 (Algorithmic Efficiency): Threshold: Prototype maintains FPR <5% on "clean" chips. Objective: Maintains FPR <1% while processing NDE data of a standard microcontroller in <60 minutes.
- MOE 3 (Adversarial Adaptability & State-Space Exploration): Threshold: Algorithmic model successfully flags a novel, previously unseen HT insertion method (provided by independent evaluation team) as an anomaly requiring human review within 72 hours of dataset ingestion. Objective: Performer's internal GAN autonomously generates and trains against a "Compound Trigger" Hardware Trojan reliant on the correlation of a defined operational state with an anomalous external input vector, unforeseen by the evaluation team.

PHASE III: DUAL USE APPLICATIONS: DoW Application: Integration into the acquisition lifecycle for systems requiring high assurance, specifically supporting deployable infrastructure, secure defense communications, and critical command and control network nodes.

Commercial Application: Transition to the Quality Assurance (QA) markets for secure financial clearinghouses, medical life-support devices, and commercial autonomous systems, where hardware-level subversion presents catastrophic safety and liability risks.

REFERENCES:

1. Department of Defense Instruction (DoDI) 5200.44, Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN), (Washington, D.C.: Department of Defense, 2012, Incorporating Change 3, October 1, 2020).
2. U.S. Government Accountability Office (GAO), Microelectronics: DoW Has Enhanced Pandemic Coordination, but Challenges Remain in Supply Chain Risk Management, GAO-23-105658 (Washington, D.C.: January 2023).
3. Mohammad Tehranipoor and Farinaz Koushanfar, "A Survey of Hardware Trojan Taxonomy and Detection," IEEE Design & Test of Computers 27, no. 1 (2010): 10-25.
4. National Institute of Standards and Technology (NIST), Platform Firmware Resiliency Guidelines, NIST Special Publication 800-193 (Gaithersburg, MD: May 2018).
5. Department of Defense, DoD Microelectronics: Vision, (Washington, D.C.: Office of the Under Secretary of Defense for Research and Engineering, 2022).
6. Department of Defense, DoD Zero Trust Strategy, (Washington, D.C.: Chief Information Officer, November 2022).
7. Defense Advanced Research Projects Agency (DARPA), Automatic Implementation of Secure Silicon (AISS) Program (Ongoing).
8. U.S. Department of Commerce, Bureau of Industry and Security (BIS), The Semiconductor Supply Chain: Assessing National Competitiveness, (Washington, D.C.: January 2022).
9. Rostami, M., Koushanfar, F., and Karri, R., "A Primer on Hardware Security: Models, Methods, and Metrics," Proceedings of the IEEE 102, no. 8 (August 2014): 1283-1295.
10. The MITRE Corporation, Hardware Common Weakness Enumeration (CWE), (McLean, VA: 2021).

KEYWORDS: Microelectronics, Hardware Trojans, AI/ML, Supply Chain Risk Management (SCRM), Zero Trust, Integrity Verification, Non-Destructive Evaluation (NDE), Generative Adversarial Networks (GAN)

DTR27TZ02-NV003 TITLE: Compact High Energy Density Capacitors For Pulsed Field X-Ray Generators

COMPONENT TECHNOLOGY PRIORITY AREA(S): Microelectronics;Advanced Materials;Directed Energy (DE)

PROJECTED CMMC LEVEL REQUIREMENT: Level 1

The technology within this topic is restricted under the International Traffic in Arms Regulation (ITAR), 22 CFR Parts 120-130, which controls the export and import of defense-related material and services, including export of sensitive technical data, or the Export Administration Regulation (EAR), 15 CFR Parts 730-774, which controls dual use items. Offerors must disclose any proposed use of foreign nationals (FNs), their country(ies) of origin, the type of visa or work permit possessed, and the statement of work (SOW) tasks intended for accomplishment by the FN(s) in accordance with section 3.5 of the Announcement. Offerors are advised foreign nationals proposed to perform on this topic may be restricted due to the technical data under US Export Control Laws.

OBJECTIVE: DTRA seeks ultra-compact, high-voltage, high energy density, capacitors and related advanced dielectric materials to support the development of advanced portable X-ray radiographic imaging systems.

DESCRIPTION: High energy density capacitors and their constituent dielectrics are vital components for multiple DoW capability needs for high voltage power supplies, Marx generators, high-power microwave sources, and other pulsed-power technologies. The Missile Defense Agency, ONR, NASA and other government agencies have funded efforts into high energy density capacitors for a variety of applications.[1] However, it is still very challenging to fabricate high energy density capacitors that reliably meet ultra-compact size constraints for miniaturized high voltage pulse power applications and in a ruggedized field-use system.

Recent prototype development of compact pulsed X-ray generators for portable radiographic imaging applications has underscored the difficulty of scaling capacitor technologies originally developed for larger directed energy and pulsed power systems down to the ultra-compact sizes needed for man-portable or small unmanned systems. Key challenges include preserving dielectric performance and high-voltage hold-off at reduced dimensions, achieving robust voltage reversal tolerance essential for Marx generator topologies, maintaining long operational lifetimes under pulsed conditions with repetition rates up to 100 Hz, and attaining high manufacturing yields with consistent quality for reliable field deployment. This topic specifically targets the development of reliable fabrication processes and advanced dielectric materials to overcome these miniaturization and ruggedization barriers for X-ray generator pulsed power applications.

DTRA seeks to develop reliable and efficient fabrication and production processes for compact high energy density capacitors.

The solution must meet the following minimum specifications:

- Outer Dimensions: No larger than 2 inches x 1 inch x 0.5 inch
- Voltage Rating: 100kV*
- Capacitance: ≥ 2nF

- Voltage Reversal Tolerance: 80%*
- Operating Environment: Dielectric Liquid or Pressurized Gas (e.g., such as SF6)
- Operating Temperature: Capable of meeting MIL-STD
- Ability to survive commercial requirements for shock and vibration (i.e. rough handling)
- Lifetime: Greater than 100,000 full-charge cycles
- Duty cycle: Up to 100 Hz
- Charge/Discharge time: Charging order of 10s of microseconds, discharge order of few nanoseconds

**Note: Operating voltage and voltage reversal are the highest priority specifications. DTRA may consider small deviations from the other minimum specifications (e.g. size) if the solution is capable of approaching or meeting the objective voltage and voltage reversal specifications below.*

Objective specifications:

- Voltage Rating: 250kV
- Capacitance: ≥ 10nF
- Capacitance Tolerance: ±10%
- Voltage Reversal Tolerance: 100%
- Operating Temperature: Capable of meeting MIL-STD
- Vibration: Capable of meeting MIL-STD
- Lifetime greater than full-charge 1,000,000 cycles

This effort shall develop a reliable manufacturing process for high energy density capacitors while maintaining the performance parameters outlined above. The proposed effort will require that developed capacitors be tested and validated in Phase 2.

PHASE I: Conceptualizing capacitor design type and proof of principle of manufacturing process. In Phase 1 of this effort, a suitable capacitor type and design will be chosen to meet the above-listed performance parameters. This decision should be informed by extensive modeling, simulation, and market research, and guided by availability of materials needed. Preference is indicated for domestically available materials. Note that while temperature and vibration ruggedization are to meet MIL-STD ranges, formal testing and certification to the MIL-STD specifications is not required during this phase.

Following the design decision, material samples will be fabricated and tested to validate performance. Evaluation of success will be weighted towards feasibility of materials to achieve the highest priority specifications: operating voltage and voltage reversal. Additionally, the offerors will define a detailed plan for a scalable prototype manufacturing process to be executed in Phase II, including equipment needs, quality control steps, and risk mitigation. The designed process should demonstrate progress towards production of capacitors that meet the defined performance criteria with particular attention to overcoming the miniaturization and reliability challenges associated with scaling from larger directed energy capacitor designs.

The Phase 1 final report should include: details for chosen capacitor design along with relevant modelling, simulation, and market research results, details of the chosen manufacturing process, and test and evaluation results of the proof-of-principle capacitor performance (including but not limited to voltage

reversal testing representative of Marx generator operation) and percentage of fabricated material samples that meet specifications via the initial process.

PHASE II: Manufacturing process execution, refinement, and scaling up of output. In Phase 2 of this effort, the manufacturing process designed in Phase 1 will be executed, refined, and scaled up with the goal of reliable capacitor output with high percentage of capacitors meeting performance specifications. The goal of this phase of the effort should be a manufacturing process with output and reliability of produced components that meet a TRL 5.

The final report for Phase 2 will include final details of the optimized manufacturing process and throughput, output capacitor specifications, and percentage of output that meets design specifications. Capacitors will be delivered to DTRA by the end of Phase II for evaluation in a representative pulsed power system for X-ray generation, as follows:

- Year 1: Fabrication of 10 prototype capacitors for testing, validation and refinement.
- Year 2: Final deliverable of up to 10 fully compliant prototype capacitors to DTRA.

PHASE III DUAL USE APPLICATIONS: Optional phase that will continue scale up and output of capacitor manufacturing process. The goal of this phase 3 work will be to produce capacitors that exceed the above listed performance specification and continue to increase the output of capacitor manufacturing while maintaining high-percentage of capacitors meeting performance specifications.

REFERENCES:

1. NASA TechPort - Project Data (https://techport.nasa.gov/view/5114)

KEYWORDS: Pulsed power; dielectric materials; capacitors; Marx generators; portable X-ray; radiography; X-ray generators; radiographic imaging; electronics; material science; high energy density; voltage reversal