Naval Information Warfare Systems Center, Pacific (NIWC Pacific)
53560 Hull Street
San Diego, CA 92152-5001

In collaboration with the
Intelligence Advanced Research Projects Activity

Broad Agency Announcement (BAA)

Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND) Program

N66001-23-S-4510

AMENDMENT 1 – 28 April 2023
Release Date: 11 April 2023

OVERVIEW INFORMATION

This notice constitutes a Broad Agency Announcement (BAA) and sets forth research of interest in the area described in detail below. The solicitation process will follow Federal Acquisition Regulation (FAR) Part 35, Research and Development Contracting, as supplemented with additional information included in this notice. Awards based on responses to this BAA will be considered the result of full and open competition.

- **Federal Agency Name:** Naval Information Warfare Center, Pacific (NIWC Pacific) on behalf of the Office of the Director of National Intelligence/Intelligence Advanced Research Projects Activity (IARPA)
- **Funding:** RDT&E (2 year)
- **Funding Opportunity Title:** Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND) Program
- **Announcement Type:** Initial Announcement
- **Funding Opportunity Number:** N66001-23-S-4510
- **Catalog of Federal Domestic Assistance (CFDA) Number:** 12.431 – Basic Scientific Research
- **Dates:**
    - Q&A Deadline Date: 25 April ~~2022~~ 2023 (2:00pm Pacific Time Zone)
    - Proposal Due Date for Initial Round of Selections: 26 May 2023 (2:00pm Pacific Time Zone)

- **Concise description of funding opportunity:** NIWC Pacific is soliciting proposals in accordance with Federal Acquisition Regulation (FAR) 6.102(d)(2), FAR 35.016 on behalf of IARPA. This notice constitutes a Broad Agency Announcement (BAA) and sets forth research of interest in improving cybersecurity by developing a novel set of cyberpsychology-informed defenses that leverage attacker's human limitations, such as innate decision-making biases and cognitive vulnerabilities. The solicitation process will follow Federal Acquisition Regulation (FAR) Part 35, Research and Development Contracting, as supplemented with additional information included in this notice. Awards based on responses to this BAA will be considered the result of full and open competition.
- **Anticipated individual awards:** Multiple awards are anticipated; the Government reserves the right to select for award all, some, one, or none of the proposals received in response to this announcement.
- **Types of instruments that may be awarded:** Procurement contracts[1]
- **Amendments:** Any amendments to this BAA will be posted via NAVWAR e-Commerce Central at https://e-commerce.dc3n.navy.mil/ (Note that this does not include a "www" prefix).
- **Agency Contact:**
  IARPA Program Email: dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov

[1] Procurement Contract: This is a standard government contract that follows the processes, format and terms and conditions as outlined in the Federal Acquisition Regulations (FAR) and supplementing Agency specific regulations.

Eric Pomroy (Primary)
Contracts Officer
Email: eric.r.pomroy.civ@us.navy.mil

Stephen Enokida (Alternate)
Contracts Officer
Email: stephen.i.enokida.civ@us.navy.mil

- **Program Manager (PM):**
  Kimberly Ferguson-Walter, Ph.D.
  Email: kimberly.ferguson-walter@iarpa.gov

- **Program Website:**
  https://www.iarpa.gov/research-programs/rescind

1. FUNDING OPPORTUNITY DESCRIPTION:

The Intelligence Advanced Research Projects Activity (IARPA) often selects its research efforts through the BAA process. The use of a BAA solicitation allows a wide range of innovative ideas and concepts. The BAA will appear on https://sam.gov/, Contract Opportunities, on the NAVWAR Contracts Directorate Website (https://e-commerce.dc3n.navy.mil/), and the IARPA website at http://www.iarpa.gov/. The following information is for those wishing to respond to this Program BAA.

This BAA is for the Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND) program. The Government is seeking innovative solutions for the ReSCIND program in this BAA. ReSCIND is envisioned to be a 45-month effort, beginning approximately November 2023.

1.A. Program Overview

Cyber attacks are increasing in quantity and severity. Some of the most sophisticated and persistent cyber attacks are primarily human-driven. However, most cyber defenses do not consider the human attributes and limitations of attackers. Furthermore, most existing defenses focus on blocking suspicious behavior and few initiate interactions with a suspected attacker to understand their attributes, skills, or goals, let alone, induce changes in their behavior.

The Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND) Program focuses on inducing or intensifying cognitive biases or other cognitive limitations to thwart cyber attackers through both novel network and host-based technologies. Rather than just attempting to detect and stop suspicious movement on the network, Offerors will propose innovative solutions to increase the effort and resources spent by cyber attackers by impacting their decision-making. The ReSCIND Program seeks novel methods that:

1. Identify, and provide evidence of, Cognitive Vulnerabilities (CogVulns) relevant to cyber attackers;
2. Understand, measure, and induce changes in cyber attack behavior and success;
3. Develop Cyberpsychology-informed Defenses (CyphiDs) impacting both early and late stage attacks;
4. Create Cyber-specific Computational Cognitive Model(s) (C3M)[2] that reflect and predict attacker behavior; and
5. Produce Adaptative Psychology-informed Defenses (APhiDs) which automate the preferred sequence of CyphiDs based on observed attacker behavior.

Cyberpsychology integrates human behavior and decision-making into the cyber domain to understand, anticipate, and influence cyber behavior. There is a vast amount of cognitive and

[2] Sun, R. (2008). *Introduction to computational cognitive modeling*. Cambridge, MA: Cambridge handbook of computational psychology. ISBN 978-0521674102.

behavioral science research that can be applied to cybersecurity to improve defensive posture. The ReSCIND program aims to develop CyphiDs that leverage an understanding of attacker decision-making, human limitations, and cognitive biases to reduce attack effectiveness. ReSCIND will rebalance the inherent asymmetry of cyber defense by exploring novel methods for manipulating attacker behavior during various phases of the Cyber Kill Chain[3].

As notionally represented in *Figure 1*, ReSCIND will provide defenders a much-needed advantage by expanding the cyber defense toolkit by specifically leveraging well-established cognitive vulnerabilities (e.g., decision-making biases, mental model heuristics) that can be intensified and manipulated to impede cyber attackers. Offerors will propose novel approaches informed by social science research and associate CyphiDs to observables (e.g., attacker attributes, situational attributes, network and host characteristics) to measurably disrupt cyber attack behavior across the various stages of the Cyber Kill Chain.

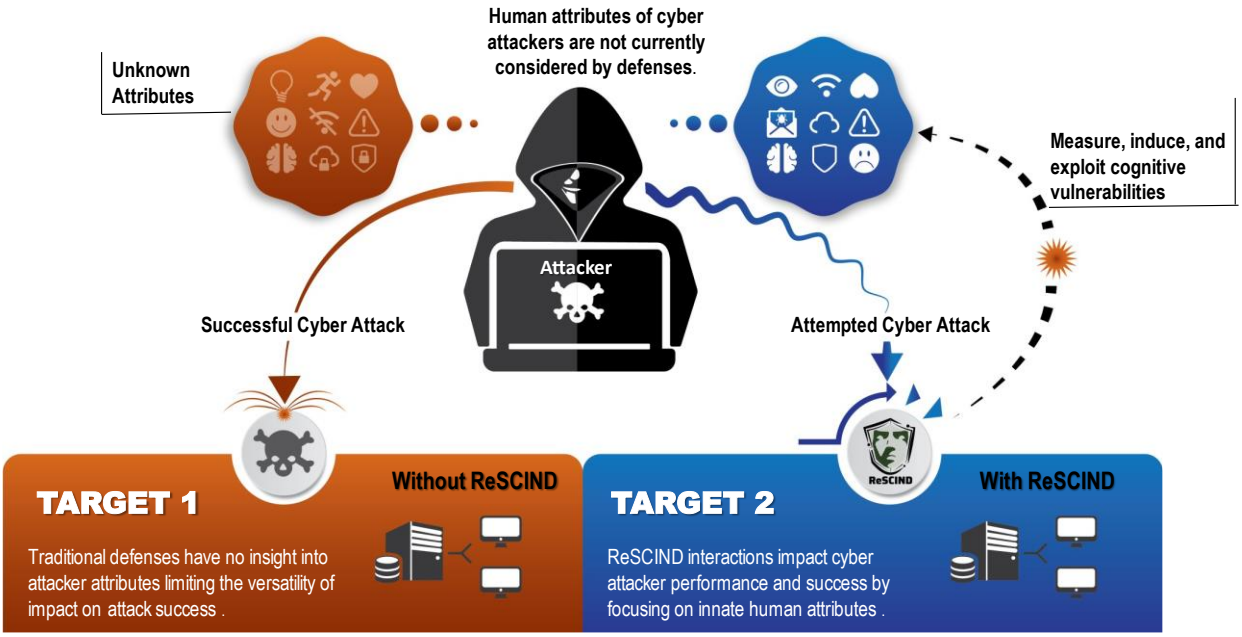


Figure 1: Notional graphic of cyber defense with and without ReSCIND

1.A.1. Technical Challenges and Objectives (TCO)

The objective of the ReSCIND Program is to impose a cyber penalty against attackers and increase the effort and difficulty for them to achieve their goals. Technical challenges and objectives include:

1. *Identify and provide evidence of CogVulns relevant to cyber attack behavior.* In the ReSCIND Program, cognitive vulnerability is an umbrella term encompassing cognitive and decision-

[3] Lockheed Martin (2015). White Paper Seven Ways to Apply the Cyber Kill Chain® with a Threat Intelligence Platform, Seven_Ways_to_Apply_the_Cyber_Kill_Chain_with_a_Threat_Intelligence_Platform.pdf (lockheedmartin.com); Ju, A., Guo, Y. & Li, T. MCKC: a modified cyber kill chain model for cognitive APTs analysis within Enterprise multimedia network. *Multimed Tools Appl* **79**, 29923–29949 (2020). https://doi.org/10.1007/s11042-020-09444-x

making biases, innate cognitive limitations, emotional or mental state, or physiological vulnerabilities that can result in reduced cyber attacker success or effectiveness. Offerors must propose their plan for novel research exploring dynamic cyber attack scenarios with skilled human participants. Observable environmental features, attacker attributes, mission context, network and host characteristics that may impact the defensive utility of selected CogVulns must be identified. Performers will:

- Establish relevance of vulnerabilities to cyber attackers, accounting for relevant differences among individuals through theoretical and experimental research.
- Design and execute empirically and statistically efficient experimental designs with cyber-skilled human participants to explore cyberpsychology in dynamic cyber attack tasks.
- Produce a CogVuln Playbook--a non-interactive structured representation that depicts hypothesized and confirmed relationships among CogVulns, bias sensors and triggers, relevant characteristics of the attacker, the network, and the external environment, and various cyber behavioral impacts (See *Table 7*).

2. *Understand, measure, and induce changes in cyber attack behavior and success.* Offerors will propose hypothesized relationships between CogVulns, bias sensors that identify and measure them, and bias triggers that create cyber situations to induce and intensify CogVulns. Performers will experimentally establish which selected CogVulns, bias sensors, and bias triggers produce a measurable effect on cyber attack behavior. Performers will:
   - Develop approaches to exploit cyber attacker CogVulns for defensive gain.
   - Understand the extent to which CogVulns may overlap and the precedent factors that lead to CogVulns in cyber-specific situations.
   - Identify novel techniques to measure, predict, and influence attacker behavior to thwart success.
   - Create bias signature(s), which maps cyber data to the presence of or increase in a specific cognitive vulnerability.
   - Develop bias sensors using data likely to be available to defenders in a realistic environment (e.g., PCAP, IDS alerts).
   - Establish bias sensor reliability and validity using established methodologies. Develop triggers (host/network manipulations) which can reliably induce or exacerbate CogVulns.
3. *Develop a collection of cyberpsychology-informed defenses (CyphiDs), each including a set of bias sensors and bias triggers focused on a cyber behavioral impact, for both early and late stages of a cyber attack.* Offerors will propose a set of CyphiDs that will demonstrate measurable impact on cyber attacker performance and success through exploitation of robust and measurable CogVulns. Sets of improved or newly created bias sensor and bias triggers will be incorporated by performers into the CyphiDs, based on the CogVulns established as an output in TCO 2. Performers will:

- Enhance the CogVuln Playbook to display the nature of the relationships between the CogVulns and CyphiDs to defensive goals and measurable impacts on cyber attack behavior.

- Implement the logic and software of cyberpsychology-informed defenses (CyphiDs) for testing in the cyber range testbed, incorporating relevant insights from the CogVuln Playbook.

- Demonstrate CyphiD efficacy for slowing or reducing the impact of cyber attack attempts.

- Develop success metrics for each CyphiD, both pre and post trigger, to evaluate the impact of the CyphiD on human-focused cyber behavior and attacker success for both early and late stages of a cyber attack.

4. *Create cyber-specific computational cognitive models (C3M) that reflect and predict attacker behavior changes in reaction to CyphiD interventions.* The models must respond to variation in CogVulns as measured by the bias sensors, such that they adapt to both raising and lowering relevant attributes using available data. The models will replicate and predict behavioral changes caused by bias triggers. Performers may elect to use their modeling to inform development of their APhiD.

    - Develop, train, and test novel cyber-specific C3Ms which reflect and predict attacker behavior, with variability dependent on presence of CogVulns.

    - Modeling efforts should also address differences in attacker behavior based on environmental features, attacker attributes, mission context, network and host characteristics, or situational factors.

5. *Produce an adaptive psychology-informed defenses (APhiD) which includes logic to automate the selection of multiple CyphiDs over time, based on observed attacker behavior.* Performers will create an adaptive defensive system that automates CyphiD selection to independently respond to cyber attacker attributes, environmental features, mission context, and network and host characteristics. Performers will:

    - Develop algorithms for APhiD to allow for automated adaptation of CyphiDs.

    - Implement the logic and software of APhiD for testing in cyber range testbed, incorporating relevant insights from the structured visual representation, and previous experimental results.

    - Provide novel generalized defenses for enterprise networks and evidenced-based use-cases, including deployment guidelines to highlight each defense's effectiveness against various real-world features (e.g., attacker attributes, mission context, network and host characteristics).

1.B. Program Phases

The ReSCIND program is a 45-month effort, comprised of three (3) phases. Proposals shall include a solution for all phases and address all technical challenges. Complete proposals will also include full experimental protocol for Phase 1 human subjects research (HSR) following the template provided in Appendix 7.A. **Proposals that do not include a complete solution for all phases or do not address all five technical challenges described above will be considered non-compliant and will not be evaluated.** The following table provides an overview of the ReSCIND program structure.

Table 1: An Overview of the ReSCIND Program Structure.

Phase	Duration	Objective
1	18 months	Identify CogVulns relevant to offensive cyber operators, including methods to induce, exacerbate, and measure each cognitive vulnerability.
2	15 months	Research and develop CyphiDs that map to observed attacker attributes and measurably disrupt cyber attack behavior across the Cyber Kill Chain and increase the negative impact on attacker performance and success.
3	12 months	Use experimental results and data from prior phases to develop APhiD (for automated selection of a combination of CyphiDs) and cyber-specific computational cognitive modeling (C3M) to reflect and predict the behavioral data provided.

The Test and Evaluation (T&E) Team will conduct several T&E events throughout the life of the program using Institutional Review Board (IRB)-approved Human Subject Research (HSR) protocols to evaluate Performer developed solutions. These will consist of controlled experiments that consider specifics of real-world cyber campaigns to balance internal and external validity. Much of this data will be made available to Performers for Research and Development (R&D) in later phases, and eventually, provided to the general scientific community. In addition, Performers will be required to conduct their own supplemental IRB-approved HSR data collection(s) and make that data available to the program. Deliverables produced by proposers must grant the Government intellectual property (IP) rights sufficient to allow the Government to conduct T&E HSR, publicly distribute performer and T&E generated datasets, and modify and deploy deliverables. Additional details on program data can be found in Section 6.

1.B.1. Phase 1

The goal of Phase 1 is to identify the CogVulns most relevant to cyber attack behavior based on foundational scientific research and cyber relevant HSR experimentation, including methods for inducing, exacerbating, and measuring the CogVulns. Phase 1 requires Performers to research and develop novel bias sensors to detect these CogVulns using cyber data, and bias triggers to induce and intensify them in a cyber situation. The ReSCIND Program encourages maximum creativity and diversity in selection of bias sensors and bias triggers; however, the scope of allowable

touchpoints is partially constrained by the data sources available in the cyber range testbed. Offerors must propose related cyber range testbed observables that they anticipate will be needed by their CyphiDs.

Bias sensors will use data accessible to cyber defenders to identify which bias trigger is most appropriate by determining the extent a cyber attacker or cyber task context is susceptible to a particular CogVuln. Bias sensors will be developed into software components for use on a network or host where the needed cyber defender data can be made available. Offerors will provide at least one established method, and optionally a context-specific alternative evaluation methodology, for T&E validation for each bias sensor delivered. The bias sensors must use data typically available to cyber defenders, while the established methodologies can use other data sources (e.g., psychometric questionnaires) or sensors (e.g., physiological devices).

Phase 1 research and development must include **two required CogVulns** selected by IARPA, loss aversion and the representativeness bias, and **at least three additional CogVulns** proposed by the Offeror. Selection criteria will include novelty, variety, relevance, quantity, scientific rigor, potential impact, etc.

For the purpose of this effort, we define the terms as follows:

- **Loss aversion**[4] is the tendency for people to strongly prefer avoiding losses to acquiring equivalent gains.

- **Representativeness bias**[5] is the tendency to overweight the representativeness of a piece of evidence while ignoring how often (e.g., its base rate) it occurs.

Performers will develop bias triggers to interact with or adapt to attackers (or portions of the network or host the attacker accesses) based on observables collected by the bias sensors and create situations in the cyber domain that induce and exploit each of the CogVulns. A bias trigger will

[4] Kahneman, D., & Tversky, A. (1979). Prospect Theory: An Analysis of Decision under Risk. Econometrica, 47(2), 263–292
[5] Kahneman, D., & Tversky, A. (1972). Subjective probability: A judgment of representativeness. Cognitive Psychology, 3(3), 430–454.

activate, induce or intensify a CogVuln. This increase should be measurable by a bias sensor or established method.

Relevant for Phase 1, Offerors should clearly describe:

- The justifications for hypothesizing that each included cognitive vulnerability is exploitable to reduce cyber attacker effectiveness, and at least one proposed bias sensor and one bias trigger that can be developed for each, although multiple triggers are preferred.
- Details on how each included vulnerability is relevant to attacker cognition and behavior, including which stage of the cyber kill chain it pertains to.
- The justifications for hypothesizing that exploiting a subset of the planned vulnerabilities will, in combination, meet required thresholds for at least one of the cyber behavioral impact metrics.
- Statistically efficient experimental design plan(s) to fully investigate the CogVulns (at least 5), bias sensors (at least one per CogVuln) and bias triggers (at least one per CogVuln).
- Designs should allow for analysis via traditional inferential statistics. In addition to quantitative analysis, HSR may include observational and qualitative studies. Sample size and participant composition must be sufficient to experimentally demonstrate that identified bias triggers are effective. Appropriate sample size will be dictated by Performer teams' experimental design plans but should be the minimum needed to show effects within the specific design. Any use of non-cyber proficient participants or non-cyber scenarios must be highly justified; effect sizes must be calculated. Proposals should justify recruitment strategies, in terms of sample size, demographics, skill levels, etc.
- Initial IRB protocols should be included as an appendix (Attachment 13) to all proposals, with Performer IRB approval expected within 3 months of program kick-off. Subsequent HSR or experimental design revisions should be handled with IRB modifications, addendums, or exemptions.

In Phase 1 Performer will develop a preliminary CogVuln Playbook. Offerors will propose a visual representation, (e.g., concept map, ontology, taxonomy) to clearly display these relationships, and include initial hypothesized relationships. CogVuln Playbooks must be driven by theory; a ―shotgun approach will be insufficient. Relevant theory from a variety of disciplines may direct the research and shall be discussed in the proposal. These playbooks will foster CyphiD development by acting as a working guide for Performer teams and be refined throughout the program. While information about individual differences should be included in the playbook, performers should assume no prior knowledge of the attacker will be provided during evaluations.

Phase 1 shall have a duration of 18 months. Additional requirements include:

- Design and execute bias discovery experiment(s) for selected and required CogVulns; experimental design and data collection must include a sufficient number of participants to calculate statistical differences (e.g., effect size, variability) with sufficient skill level to

generalize to an expert population. Sample size efficient designs are acceptable; number of participants, skill level, and recruitment plan must be justified.

- Offerors should account for a sufficient number of cognitive vulnerabilities, bias sensors, and bias triggers to account for potential construct failure.
- Provide established methods and evaluation thresholds to determine ground truth of presence of each of the CogVulns.
- Prepare cyber range testbed provided by T&E for inducing and measuring performer CogVulns, and perform self-testing for bias sensors and triggers.
- Ethics review (e.g., Institutional Review Board (IRB)) approval or exemption will be required. Performer teams must have access to an ethics review board, and expertise on navigating the process.

1.B.2. Phase 2

The goal of Phase 2 is to develop novel Cyberpsychology-informed Defenses (CyphiDs) to impose a cyber penalty and thwart attacker success across the Cyber Kill Chain. A set of bias sensors and bias triggers developed for a specific cognitive vulnerability, or cognitive vulnerability cluster, will be considered a CyphiD as shown in *Figure 2*. CyphiDs consist of one or more bias sensors which measure the presence of a CogVuln, logic to determine based on bias sensor output (and other cyber data, as needed) which bias trigger to utilize (if any), and one or more trigger(s) which create a cyber situation to induce, exploit, or intensify the CogVuln. In Phase 2, Performers will develop the CyphiD software and logic that links sensors and triggers. Offerors must propose a design for proposed CyphiDs, including logic, proposed mappings of bias sensors to bias triggers, as well as cyber data required for the sensors, and touchpoints needed for the triggers. For each CyphiD, offerors must propose success metrics and details on how to measure behavioral impact for each of the 7 cyber behavioral impacts listed in *Table 5*. Offerors will also propose which observable cyber data will be required, what attack scenarios are being targeted, and any other CyphiD-specific information that is needed to prepare the testbed and T&E experimental design to evaluate performer solutions.

Additional bias sensors and bias triggers may be developed in Phase 2 based on Phase 1 experimental findings or additional HSR. Offerors should discuss how experimental design(s) will allow for quick additional HSR in Phase 2, if needed. Performer teams will need to produce at least 5 CyphiDs that impact early kill chain attacker behavior, and at least 5 CyphiDs that impact late kill chain behavior (late is defined as post exploitation). A CyphiD that is effective for both early and late kill chain behavior, may count for both categories. Teaming is strongly encouraged to accomplish these goals. Performers will create a simple, minimally-interactive, custom dashboard to visually assist defenders in understanding the findings of the sensors (i.e., the degree of each cognitive vulnerability measured) and the impact of the CyphiDs. Phase 2 metrics will focus on achieving a medium effect size across multiple areas of defender goals. It is not expected

that each CyphiD meet each cyber behavioral impact requirement threshold (See *Table 4*), but rather the Performer's collection of CyphiDs meets each at least once.

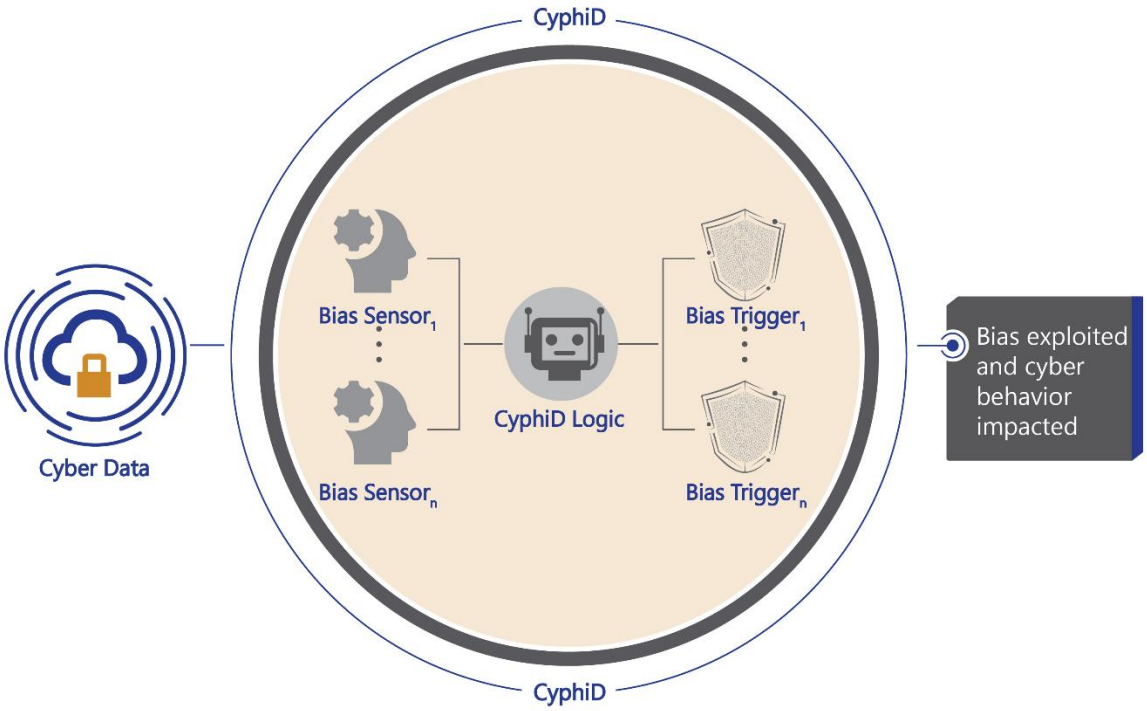


Figure 2: Notional CyphiD Graphic: Bias sensors, bias triggers, and logic combine to form CyphiDs. Each CyphiD focuses on achieving a desirable cyber behavioral impact.

In Phase 2, Performers will continue to update their CogVulns Playbook and implement relevant portions into their software to demonstrate under which conditions a particular CyphiD should be used for the seven cyber behavioral impacts. Attacker attributes and/or situational factors can be observed by bias sensors and exploited by the CyphiDs, while network and host characteristics can be altered by the bias triggers. These features should be included in the structural representation and examined throughout the research.

Self-testing of CyphiDs within the provided cyber range test bed environment will be performed iteratively by Performers in each performer's dedicated instance of the cyber range testbed, with results and interpretation of results delivered to IARPA. A leaderboard will be provided to track

the successes of each team's CyphiDs against the program metrics and will contain both self-testing results, and T&E event results.

Phase 2 shall have a duration of 15 months. Additional requirements include:

- Improve (and/or create new) bias sensors and bias trigger to achieve Phase 2 program metrics.
- Request and justify any additional cognitive vulnerability-specific metrics to be included for HSR T&E events.
- Fully document each CyphiD (which will be used across all Performers teams during Phase 3).

1.B.3. Phase 3

The goal of Phase 3 is to automate, model, and improve research findings from previous phases, while reaching higher effect sizes. Performers will develop an adaptive psychology-informed defense (APhiD), which automatically selects the appropriate combination or sequence of CyphiDs over time (See *Figure 3*). Performers will also research and develop novel Cyber-specific Computational Cognitive Models (C3Ms) based on experimental findings to date; successful models will reflect and predict cyber attacker behavior with sensitivity to various conditions listed in the static visual representation and adjust based on bias sensor measurements of each CogVuln.

In Phase 3, all Performers will be working from an integrated CogVuln Playbook provided by the IARPA team that is based on elements from each Performer team's Phase 1 and 2 contributions. Performers will incorporate relevant portions of the CogVuln Playbook to provide a priori knowledge to the APhiD and determine situations in which a particular CyphiD would be selected,

including various attacker attributes, attacker behaviors, network and host characteristics, situational attributes, and/or time factors.

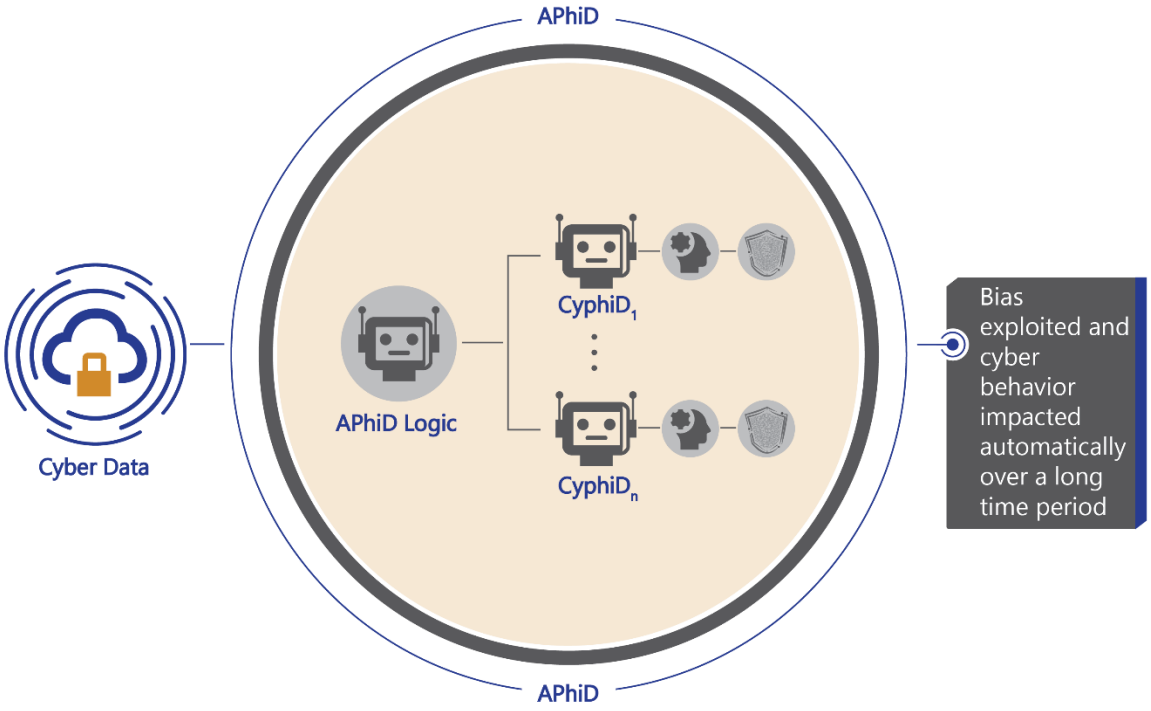


Figure 3: Notional APhiD Graphic: Multiple CyphiDs combined with logic determining which to use at each point in time form an APhiD.

APhiD must run autonomously by creating intelligent algorithm(s) (e.g., expert system, game theory, artificial intelligence, rule-based system) to select the optimal combination or sequence of CyphiDs throughout an extended period of time. IARPA will provide Performers teams with an annotated and labeled dataset for training their APhiD, as well as all available Performers team CyphiDs for optional inclusion. Performers will use the dataset(s) provided by IARPA, as well as Performers data and findings from their Phase 1 HSR, to develop C3Ms and APhiD. Offerors must propose an initial design, implementation, and self-testing plan for their APhiD to automate CyphiD usage and improve cyber behavioral impact.

The C3Ms will focus on the CogVulns examined by the Performers in Phase 2. The anticipated changes in behavior caused by each of the Performer's CyphiDs should be handled by at least one model. Models must use ecologically relevant sensor measurements, which can be reasonably obtained in cyber security environments such as security operations centers (SOCs). C3Ms should model an adjustable degree of CogVuln on a continuous scale, such that the model behavior changes based on the degree of CogVuln presence selected in the model. Excessively complex non-linear models are discouraged due to overfitting concerns. Performers may include their C3M(s) as part of their APhiD logic. Offerors must propose an initial design, implementation, and

self-testing plan for the C3M(s) to recapitulate the pattern of human behavior as it relates to decision-making and CogVuln-specific behavioral changes in a cyber attack scenario.

Phase 3 shall have a duration of 12 months. Additional requirements include:

- Store, process, and understand the large-scale HSR dataset provided by IARPA
- Provide CyphiDs with documentation across all Performer teams.
- Validate APhiD with self-testing in cyber range testbed and submit findings and interpretation.
- Develop simple, minimally-interactive, custom dashboard to visually present and help end-users understand how sensors, triggers, and APhiD are working and their impact on attack behavior.
- Develop a sufficient number of C3M(s) to define and emulate all the CogVulns included in CyphiDs by the Performer during Phase 2.
- Perform iterative testing of cognitive models against the training data provided, report all data and interpretations of data and analyses to IARPA.
- Provide updates to the common CogVulns Playbook based on findings and interpretation of results.

1.C. Team Expertise

To address the combination of challenges presented by ReSCIND, **collaborative efforts and teaming arrangements among Offerors are strongly encouraged**. It is anticipated that teams will be multidisciplinary and may include expertise in one or more of the disciplines listed below. This list is included only to provide guidance for the Offerors; satisfying all the areas of technical expertise below is not a requirement for selection and unconventional or innovative team expertise may be needed based on the proposed research. Specific content, communications, networking, and team formations are the sole responsibility of the participants. Proposals should include a description and the mix of skills and staffing that the Offeror determines will be necessary to carry out the proposed research and achieve program metrics.

- Behavioral science and cognitive psychology
- Defensive cyber operations
- Cognitive modeling
- Cyber attack modeling
- Penetration testing/red teaming and adversary emulation
- Artificial intelligence and adaptive systems
- Statistical data analysis and mathematical modeling
- Software development and engineering
- Criminology
- Cognitive and neurosciences
- Human factors engineering
- Human computer interaction
  Computer security and network security

1.D. Program Scope and Limitations

Proposals shall explicitly address all the following:

- **Underlying Theory**: Proposed strategies to meet program-specified metrics must have firm theoretical bases that are described with enough detail that reviewers will be able to assess the viability of the approaches. Proposals shall properly describe and reference previous work upon which their approach is founded.
- **Research & Development Approach**: Proposals shall describe the technical approach to meeting program metrics.
- **HSR Protocols**: Proposal shall describe the approach for recruiting human subjects and ensuring ethical treatment and responsible data handling in Attachment 13 (See Appendix 7.A template). Experimental procedures must discuss and justify design decisions supporting or limiting internal, external, ecological and construct validity. Protocols for the ReSCIND program should be new IRB submissions, and not modifications of an existing protocol.
- **IRB Approval**: Proposal shall describe the approach for, and experience in, obtaining timely IRB approval for all phases of experimentation and any required modifications; Performer teams must ensure IRB approval from their IRB authority as well as government concurrence prior to conducting HSR.
- **Data Analysis Strategy**: Proposals shall describe how HSR protocols will yield data that can meet program metrics through both qualitative and conventional statistical analyses

and articulate the reasoning behind any nonparametric or otherwise atypical analytical approaches. Data collection, storage, labeling and analysis plans shall be included.
- **Technical Risks and Mitigations**: Proposals shall identify technical risks and proposed mitigation strategies for each.
- **Software Development**: Proposals shall describe the approach to software architecture and integration.

The following areas of research are **out of scope** for the ReSCIND program:

- Research that does not have strong theoretical and experimental foundations.
- Research that cannot be implemented to facilitate identification or development of a CyphiD.
- CyphiDs or APhiDs that require the live access to the Internet.
- Bias sensors or triggers designed to solely target a non-human cyber attacker.
- Bias triggers that do not have a cyber behavioral impact.
- Technologies focused solely on cyber deception or traditional cyber defenses.
- Attacker activity that occurs prior to initial network access (e.g., OSINT target research)
- Attacker activity relying on interaction with live humans (e.g., social engineering, phishing), including defenders or users.
- Hardware solutions.
- Attribution of specific ATPs or cyber actors; techniques solely focused on intelligent gathering.
- Approaches that require access to classified information or data. All Performer research will be strictly unclassified.
- Design and development of a new interactive human machine interface (HMI).
- Development of a simulated or emulated cyber range testbed is out of scope.
- CyphiDs that only work on a simulated network and not an operational network.

1.E. Test and Evaluation (T&E)

T&E will be conducted by an independent team of FFRDC, UARC or Government staff carrying out evaluation and analyses of Performer research deliverables using program tests and protocols. In addition to independent T&E, the program will regularly gauge interim progress of Performer research activities towards ReSCIND objectives and target metrics using T&E results measured and reported by the Performer teams themselves. The ReSCIND Program will pursue rigorous and comprehensive T&E to ensure that research outcomes are well characterized, and deliverables are aligned with program objectives. Such T&E activities will not only inform Government stakeholders on ReSCIND research progress but will also serve as valuable feedback to the Performers to improve their research approaches and system development. The ReSCIND Program will work closely with Government leaders in cyber operations and cyberpsychology to continually refine and improve T&E methodologies.

A series of HSR experiments will be conducted by T&E throughout the program to test Performer solutions and generate datasets. These HSR experiments will be used to evaluate the effectiveness of the Performer's capability at various stages of the program. Performers will also be required to demonstrate execution of their developed capabilities (i.e., bias sensors, bias triggers, CyphiDs,

APhiDs) using the provided cyber range testbed (e.g., an independent T&E-hosted and configured instance of CyberVAN). This DoD-funded cyber range testbed will provide T&E the framework for creating a robust and realistic testbed for the program. Performer teams will not access this T&E instance, nor be provided full details of the T&E configuration, which will be used to independently evaluate Performer deliverables. An instance of CyberVAN will be made available to Performers 2 as Government Furnished Information (GFI) for self-testing of functionality and integration by Phase 1 Month 10 and should not be relied on for Performer HSR. Information provided in proposals about necessary network and host characteristics, data sources, and trigger touchpoints for the cyber range testbed will be used by T&E for configuration changes.

Phase 1*:* To meet the goals of phase 1, Performers will conduct their own HSR in Phase 1; this will occur independently from the Program's cyber range testbed. Phase 1 Performers HSR should be a proof of concept demonstrating in which cyber attack task(s) each bias trigger is most effective. Performers' initial experimental designs will be assessed with a T&E rubric by a group of subject matter experts (SMEs) as a midterm T&E event for Phase 1.

The final experimental execution, data analysis, and interpretation of findings done by Performers will be evaluated with a T&E rubric by a group of SMEs as the final T&E event for Phase 1. The data analysis must include both qualitative and quantitative results. Raw and curated data collected by Performers to measure effect size must be provided to T&E for validation. Bias sensors and triggers will be evaluated for integration into the cyber range testbed. Additionally, the accuracy of the bias sensors will be evaluated by examining the extent to which bias sensor results reflect previously established and validated measures, which refer to approaches that are widely used and well-accepted among related fields of research to accurately measure the outcome of interest. The bias sensors must use data typically available to cyber defenders, while the established methodologies can use other data sources and sensors. T&E may also include additional established methods and/or independent approaches as part of their evaluation. The T&E team will validate that bias triggers have the desired behavioral effect on attacker behavior (i.e., induce, increase/decrease a specific CogVuln) by examining effect size.

Phase 2: To meet the goals of Phase 2, controlled HSR experiments with cyber experts will be executed by T&E. Phase 2 evaluation consists of large-scale HSR with cyber attack experts to demonstrate statistical and practical significance of the CyphiDs. The first T&E event will focus on Early Kill Chain CyphiDs (reconnaissance though initial exploitation), and the later event on the late Kill Chain CyphiDs (post exploitation). As part of T&E, cyber experts will be directed to perform tasks such as: network reconnaissance and penetration, target discovery and selection, delivery, exploitation, persistence, defensive evasion, command and control, pivoting, privilege escalation, credential access, lateral movement, collection, exfiltration, and other standard penetration testing tasks. Phase 2 T&E will also include evaluation of new (or improved) bias sensors; if any new HSR data is collected by Performers, it will also be provided to T&E and effect sizes calculated.

Phase 3: To meet the goals of Phase 3, T&E evaluation will focus on the predictive power of the models and generalizability of APhiDs. T&E will use typical model fitting metrics (See *Table 5*)

to examine how C3Ms reflect the data provided and will examine the predictive power of the C3M using a testing dataset.

To evaluate the Adaptative Psychology-informed Defenses (APhiDs) in Phase 3, an online open prize competition in the format of a capture-the-flag (CTF) T&E event will be held to test Performer solutions against a wider range of attack behaviors and attacker attributes.

Experimental analysis results will be utilized to iteratively improve the cyberpsychology-inspired methods and techniques. Performers are encouraged to work with T&E and propose and justify additional data to be collected, CogVuln specific metrics needed, CyphiD/APhiD specific flags, and additional characteristics of the participants to be measured and examined during T&E events, which may be included at the discretion of the IARPA PM. Additional relevant and reasonable observables, variables, or metrics that are supported by theory or prior research will be favorably evaluated. The IARPA Team may conduct other supplemental evaluations or measurements at any time and without notice.

1.F. Program Data

Across phases, the T&E team will conduct HSR (including data collection/curation) using cyber experts. These experiments will collect cyber attacker behavior and performance data, though realistic simulated cyber attack scenarios. During Phase 1, the only data the Performers will obtain is the data the Performers generate themselves through their bias discovery experiments. During Phase 2, Performers will again rely on the data they have collected through HSR and self-testing within the testbed. Results from the Early Kill Chain T&E Event will be provided to Performers during Phase 2 as GFI and should be used to improve their deliverables for the Late Kill Chain T&E Event. During Phase 3, the government will provide Performers, as GFI, a more fully curated dataset created by T&E from the Phase 2 HSR to support both APhiD decision-making and C3M development. At Phase 3 kick-off Performers will be required to share their CyphiDs across teams to expand the collection of available options for APhiD selection.

Table 2 describes the data that may be collected by T&E. An updated list of available planned data will be made available at Phase 1 kickoff. Offerors must notate any additional data requested relevant to the specific CogVulns, CyphiDs or APhiDs they propose. Performers will develop CyphiDs and APhiDs for a standard IT network with typical enterprise targets such as, Windows or Linux operating systems, Domain Controller, Git Repository, routers, development workstations, database and file share servers, multiple subnets and target environment will not include removable media, live (benign) users or administrators.

Table 2: Examples of the Types of Data that Could be Collected in the T&E Environment

Data Type	Data Example
Scenario Data	Subject ID, date, day, condition, environment, daily start/end time, breaks/lunch, subject start/end time, cyber task end time, subject time on task, screen capture

Environment Data	Subject IP, target IPs, target host configuration (e.g., OS, ports), host name, vulnerabilities
Network Data	Packet ID, PCAP, netflow, PCAP timestamp, destination IP, PCAP size, source IP, destination IP, port, timestamp
Host Data	Process logs, file touches, services, process history, file data, system & application host logs
User Data	User accounts, access logs, privilege, user files, login attempts
Attack Data	Exploit timestamp, exploit name, exploit CVE, success/failure
Alert Data	Signature ID, IDS alert description, CVE, severity, target IP, timestamp, custom alerts
Forward Progress	Flags captured, data exfiltrated, lateral movement, privilege escalation
Self-Report Data	Timestamp, self-reported vulnerabilities identified, self-reported exploit attempts, self-reported success/failure, Red Team Briefing
Individual Measures	Bias-specific questions, Reported Cognitive State, Experience, Demographics, General Decision-Making Style Inventory (GDMSI), Indecisiveness Scale (IS), Big Five Inventory (BFI-44), custom questionnaires
CyphiD Data	To be included in proposal by Offerors
APhiD Data	To be included in proposal by Offerors

Performers can expect solutions to defend against cyber attackers using standardized, openly available cyber attack tools including Kali Linux and included toolsets such as Metasploit, Armitage, Burpsuite, etc. Attackers will be given high level goals but will not be told how to execute their attack or strategies to compromise the target network, so any malicious activity possible on the network may be expected.

Data that is out-of-scope for collection and use in this program include: OSI Layer 1 data, hardware or infrastructure components, OSINT, social engineering, Internet of Things (IOT), Industrial Control Systems (ICS) or SCADA devices, mobile/cellular devices, close access or physical interactions, RFID, radio frequencies, two-factor authentication, and tactical networks. CyphiDs will not have real-time access to the internet during evaluations.

Performers will be provided attack scenarios to focus on during Phase 1 kick-off. These scenarios will include enterprise network layout and devices and focus on attack scenarios described in Table 3.

Table 3: Descriptions of Various Cyber Attack Event Types

Cyber Attack Event Type	Description

Software Supply Chain Attack	Software supply chain attacks including, supply chain espionage, malware injected into software development process, and deployment into target domain, compromising software development infrastructure, and compromising certificate update and signing process.
Data and Intellectual Property (IP) Theft	Activities taken to identify and strategically exfiltrate data and intellectual property related to mission objectives.
Malicious Data Modification	Data modification on target environment with the objective of triggering external events related to system access log files, system alerts, notification triggers, or restricting role-based access control.
Denial of Service	Targeted denial including placement of ransomware on critical targets, distributed denial of service (DDoS) of a specific service, and targeted reuse of these attacks toward final objective.

1.G. Program Metrics

Achievement of metrics is a performance indicator under IARPA research contracts. IARPA has defined ReSCIND program metrics to evaluate effectiveness of the proposed solutions in achieving the stated program goal and objectives and to determine whether satisfactory progress is being made. The metrics described in this BAA are shared with the intent to scope the effort, while affording maximum flexibility, creativity, and innovation to Offerors proposing solutions to the stated problem. Proposals with a plan to exceed the defined metrics in one or more categories are desirable, provided that all of the other metrics are met, and provided that the proposals provide clear justification as to why the proposed approach will be able to meet or exceed the enhanced metric(s).

The final ReSCIND T&E protocols and evaluation methodology are currently under development; further details will be provided at program kickoff. Program metrics may be refined during the various phases of the ReSCIND program; if metrics change, revised metrics will be communicated in a timely manner to Performers. The evaluation methodology may be revised by the Government at any time during the program lifecycle to better meet program needs.

Phase 1 will include two types of metrics: Statistical metrics and qualitative metrics (*Table 4*). Statistical metrics are designed to establish external validity and efficacy of bias sensors and bias triggers. Qualitative metrics are designed to establish internal validity of the Performers' experimental design strategies using structured expert evaluations. Effect size, which is sample size agnostic, will be measured using Cohen's d; d=M1-M2/SD[6] for parametric data, with Cohen's d analogs[7] used in the case of non-parametric data. The degree to which the bias sensors overlap

[6] Vogt, W.P. & Johnson, R. B. (2015). The SAGE Dictionary of Statistics & Methodology: A Nontechnical Guide for the Social Sciences, 5th Ed., Sage Publications, Inc

[7] Wilcox, R. (2019). A Robust Nonparametric Measure of Effect Size Based on an Analog of Cohen's d, Plus Inferences About the Median of the Typical Difference. Journal of Modern Applied Statistical Methods, 17(2), Article 1.

with the validated measure(s) will be measured using standard deviation (SD); SD=$\sqrt{\sum}(X-\mu)2/N$[8]. For Phase 1, an effect size approaching medium is expected. In cases where sensors do not converge with validated methodologies, using alternative evidence of efficacy may be proposed by Performers and evaluated by the T&E team using the SME rubric or other strategies. ~~Bias~~ T&E will account for different interpretations of CogVulns that may be cyber-relevant (e.g., state vs. trait manifestations of the constructs; cultural variations that may exist) in their evaluations of Performer solutions. Deliverables must include all details required to replicate data analysis performed.

Table 4: Statistical and Qualitative Metrics Used in Phase 1

Statistical Measures	**Phase 1 Target**
External validity check	Bias sensor: within 1.5 SD of baseline
Higher effect size	Bias trigger: Cohen's $d \geq 0.3$
Qualitative Metric	**Phase 1 Evaluation**
Manipulation and validity check	Experimental design: SME Rubric

Phases 2 and 3 include two types of metrics: Behavioral metrics and statistical metrics (*Table 5*). Behavioral metrics are designed to establish that specified defender goals are achieved to decrease cyber attacker success and effectiveness. Offerors will propose how each behavioral metric can be determined based on performer-specific CyphiD designs. For example, for a CyphiD targeting the exfiltration phase of a cyber attack the "Rate of Attack Success" metric could examine the proportion of attempts that were successful versus those that were unsuccessful (i.e., if 10 files were successfully exfiltrated in the control condition, then a successful CyphiD would reduce that to 5 files). While the "Progress Towards Goal" metric could examine how the use of a CyphiD changed which phase of the Cyber Kill Chain was reached (i.e., if a participant reached the exploitation phase 10 times when the CyphiD was absent, but only 5 times when the CyphiD was used). T&E will consider performer proposed behavioral metrics, which may be modified by T&E and/or combined with additional evaluation metric calculations. Demonstration of cyber behavioral impact compared to a control condition (without CyphiDs but including traditional cyber defenses) will indicate that Performer solutions are achieving ReSCIND metrics in Phase 2 and will be improved with automation in Phase 3. Additional comparisons within subjects will also be performed in all instances where theoretically or analytically appropriate. Medium levels of effect size will be used to evaluate Phase 2 performance, while an effect size approaching high is expected in Phase 3Each CyphiD must meet at least one cyber behavioral impact threshold; the collection of a Performer's CyphiDs will seek to meet all targets. Phase 3 cognitive computational models will be evaluated by testing model fit and predictive ability against datasets collected

[8] Vogt, W.P. & Johnson, R. B. (2015). The SAGE Dictionary of Statistics & Methodology: A Nontechnical Guide for the Social Sciences, 5th Ed., Sage Publications, Inc

throughout the phases using root mean squared error (RSME= $\sqrt{[\ \Sigma(Pi - Oi)2 / n\ ]}$)[9] for continuous output. Other standard model efficacy measures may be used by T&E where appropriate.

Subjective measures for CyphiDs and APhiDs will also be considered such as: usability, adoptability, security, coverage of attack phases and TTPs, and potential interference with benign users or devices.

Table 5: Cyber Behavioral Impact and Statistical Metrics for Phases 2 and 3

Cyber Behavioral Impact	Notional Behavioral Metrics	Phase 2 Target	Phase 3 Target
Decrease Rate of Attack Success	Number of goals completed	50% ≤ control	APhiD: 10% improvement on best team's Phase 2 results for each cyber behavioral impact
Decrease Progress Towards Goal	Number of sub-tasks completed	50% ≤ control	
Decrease in Time Until Detection	Time until first alert	50% ≤ control	
Increase in Detectability of Attacker	Ratio of true positive alerts	50% ≥ control	
Increase Time to Task Completion	Duration of time to complete task	50% ≥ control	
Increase Attacker Cognitive Effort Spent	Number of strategy changes per task	50% ≥ control	
Increase Attack Resources Wasted	Number of attempts per task	50% ≥ control	
Cyber Behavioral Impact	**Statistical Metrics**	**Phase 2 Target**	**Phase 3 Target**
For all 7 Cyber Behavioral Impacts	Higher effect size	CyphiD: $d \geq 0.5$	APhiD: $d \geq 0.7$
	Predictive power	N/A	Models: RMSE ≤ 0.2

1.H. Program Waypoints, Milestones, and Deliverables

Waypoints, Milestones, and Deliverables are established from the program's onset to ensure alignment with ReSCIND objectives, organize research activities in a logical and reportable manner, and facilitate consistent and efficient communication among all stakeholders – IARPA, ReSCIND T&E, USG Stakeholders, and Research Performers (see *Table 6*). A schedule of anticipated key program Milestones and Deliverables is shown in *Figure 4*. Performers shall provide results from self-testing to be included in ReSCIND leaderboard. T&E results may also

[9] Vogt, W.P. & Johnson, R. B. (2015). The SAGE Dictionary of Statistics & Methodology: A Nontechnical Guide for the Social Sciences, 5th Ed., Sage Publications, Inc

be included. Delivered reports and documentations shall be submitted as Microsoft Word file(s), and HSR data shall be submitted as CSV file(s).

Table 6: Table of ReSCIND Program Deliverables and Milestones

Phase	Month	Event	Description	Comments	Deliverables
1-3	all	Waypoint	Monthly Status Report	Due on 15th of each month	MSR
1-3	all	Waypoint	Progress and Status Meetings	Monthly teleconference with IARPA Team; additional as needed	Meeting Notes and action items
Phase 1					
1	1	Waypoint	Phase 1 Kickoff	Location TBD	N/A
1	2	Deliverable	IRB Submission	Any IRB modifications with approval must be submitted throughout the program	All IRB Docs
1	2	Deliverable	Privacy Plan v1.1	Submitted for IARPA approval	Report
1	3	Deliverable	CogVuln Playbook	Updated to focus on aspects included experimental design(s)	Report, visualization
1	3	Waypoint	Performer IRB Approval	Initial approval from performer IRB(s)	IRB Approval Document
1	4	Deliverable	Draft Experimental Design(s)	Performer methods, materials, analysis plan	Report
1	5	Waypoint	Site Visit	Onsite at Performer location.	N/A
1	5	Milestone	T&E Event	SME evaluation of draft experimental designs	N/A
1	5	Waypoint	Full IRB Approval	Including DoD review and any cross institutional agreements	IRB Approval Document
1	6	Deliverable	Final Experimental Design(s)	Includes established methodologies for external validation.	Report
1	9	Waypoint	PI Review Meeting	N/A	N/A
1	10	Deliverable	Bias Sensors and Triggers Materials	For mandatory CogVulns	Software, Documentation, Testing Procedure

Phase	Month	Event	Description	Comments	Deliverables
1	11	Deliverable	Experimental Results	Data analysis and interpretation of results for mandatory CogVulns	Report, Data, all Experimental Materials
1	11	Waypoint	Site Visit & Demo	Onsite at Performer location	Demo of completed experiments
1	14	Deliverable	Bias Sensors and Triggers Materials	For additional CogVulns	Software, Documentation, Test Suite
1	15	Waypoint	Site Visit & Demo	Onsite at Performer location.	Demo on all CogVulns
1	15	Deliverable	Experimental Results	Data analysis and interpretation of results for additional CogVulns	Report, Data, all Experimental Materials
1	16	Waypoint	T&E Event	SME evaluation of final experimental results	N/A
1	17	Deliverable	Phase 1 Final Report	Final Phase 1 Report; include Phase 2 implementation plan	Final Report
1	17	Deliverable	Bias Sensors and Triggers Materials	Includes any changes	Software, Documentation
1	18	Waypoint	End of Phase 1 PI Meeting & Demo	In DC. Will include demo for stakeholders.	N/A
Phase 2					
2	19	Waypoint	Phase 2 Kickoff	Takes place in San Diego	N/A
2	19	Deliverable	IRB Amendments for Additional HSR	Additional HSR should focus on same CogVulns	All IRB Documentation
2	20	Deliverable	Experimental Design(s)	Experimental design(s) for all additional HSR.	Report
~~1~~ 2	~~2~~ 21	Deliverable	Privacy Plan v2.0	Submitted for IARPA approval	Report
2	21	Waypoint	Full IRB Approval for Additional HSR	Approval (including DoD review) must occur prior to HSR execution	IRB Approval Document
2	24	Deliverable	Report on completed additional HSR	Data analysis and interpretation of results	Report, Data, all Experimental Materials
2	24	Waypoint	Site Visit & Demo	Onsite visit to Performer location.	Early Kill Chain demo in testbed

Phase	Month	Event	Description	Comments	Deliverables
2	25	Deliverable	Updated Bias Sensors and Triggers	Source code, and executables, along with setup and testing documentation.	Software, documentation, testing
2	25	Deliverable	Early Kill Chain CyphiDs	Integratable into cyber range testbed; Include test suite	Software, Executables
2	26	Waypoint	PI Meeting	Location TBD	N/A
2	26-27	Waypoint	T&E Event	Early Kill Chain HSR	N/A
2	28	Waypoint	Phase 2 Full IRB Approval/Exemption	To handle and analyze Phase 2 HSR data collected by T&E Team	IRB Document
2	30	Deliverable	Deliver Late Chain CyphiDs	Integratable into cyber range testbed; Include test suite	Software, Executables
2	30	Waypoint	Site Visit & Demo	Onsite visit to Performer location.	Late Kill Chain demo in testbed
2	31	Waypoint	T&E Event	Late Kill Chain HSR	N/A
2	32	Deliverable	Updated CogVuln Playbook	Based on additional HSR and T&E event results	Report, visualization
2	33	Waypoint	PI Meeting	Location TBD	N/A
2	33	Deliverable	Final Report on all CyphiDs	Based on all T&E results and HSR to date.	Final Report, updated software
Phase 3					
3	34	Waypoint	Phase 3 Kickoff	Takes place in San Diego	N/A
~~1~~ 3	~~2~~ 36	Deliverable	Privacy Plan v3.0	Submitted for IARPA approval	Report
3	36	Deliverable	Implementation plan for APhiD	Includes algorithms to select the combination/sequence of CyphiDs	Report
3	36	Deliverable	Implementation plan for C3Ms	Includes algorithms to model cyber behavior and CogVulns	Report
3	37	Waypoint	Site Visit	Onsite to Performer location.	N/A
3	39	Waypoint	PI Meeting	In D.C.	N/A
3	42	Deliverable	Deliver APhiD	Includes visualization, source code, documentation, libraries, binaries	Software, executable
3	42	Waypoint	Site Visit & Demo	Onsite to Performer location.	Demonstrate APhiD and C3M

Phase	Month	Event	Description	Comments	Deliverables
3	43	Milestone	T&E Event	Online CTF Prize Competition	N/A
3	44	Deliverable	Deliver final C3Ms	Includes dashboard, source code, documentation, libraries, binaries	Software, executable
3	44	Waypoint	T&E Event	Evaluation of C3M	N/A
3	45	Report	Final Report	Any updated software and documentation are due.	Final Report
3	45	Waypoint	Final PI Meeting & Demo	Takes place in D.C.	Demo for stakeholders

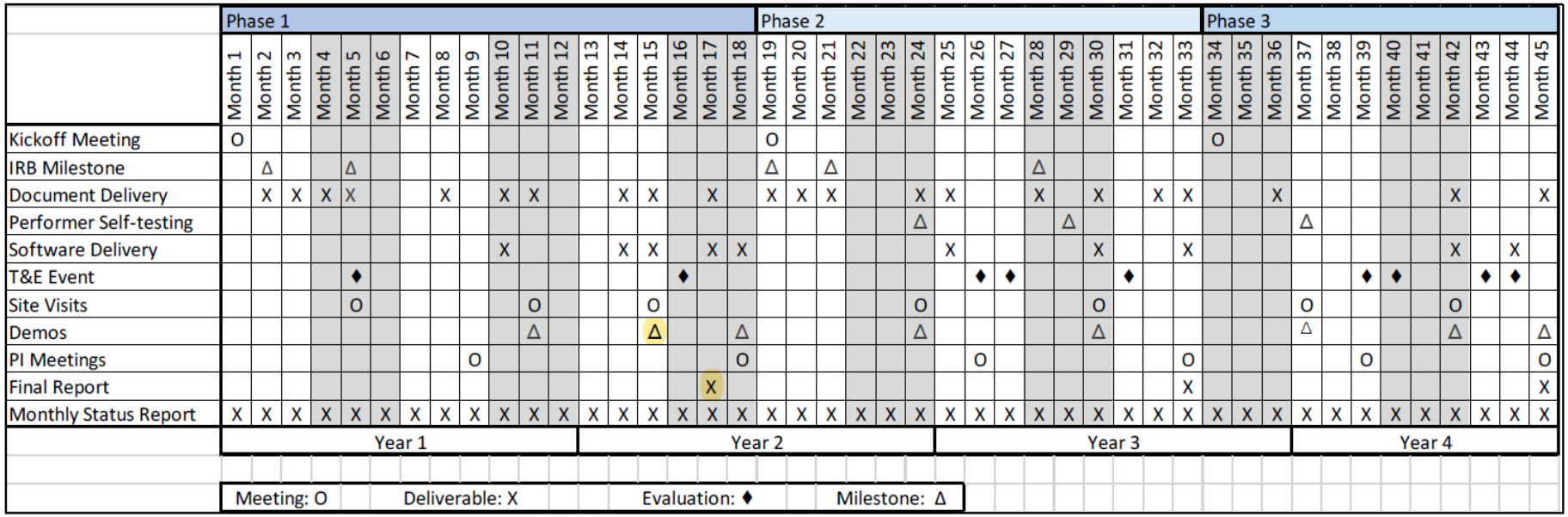


Figure 4: Graphical Schedule of ReSCIND Program Deliverables and Milestones

1.I. 9 Software Deliverable Formatting

The ReSCIND Program will use a standardized API for all software deliverables and evaluations. The first version of the ReSCIND API will be provided to Performers at the Phase 1 Kickoff Meeting and updated periodically thereafter. The API will define function calls, data structures, and data pipeline and management for CyphiD and APhiD integration, testing, and operating and evaluating ReSCIND software in a standardized manner. A secondary API may be necessary for sensor registration to the testbed itself. The API will be as software and hardware agnostic as is practical, to ensure Performers can freely develop solutions according to skill and vision.

Each team is required to include among their key personnel a Lead System Integrator (LSI) who shall be responsible for preparing software deliverable subcomponents, modules, and systems, performing quality control of deliverable(s), and assisting the T&E team with aspects of integrating key components into the primary ReSCIND testbed. The LSI will also oversee communication and coordination across a Performer's research teams including subcontractors, if applicable, to ensure research products are functional and following software coding best practices and requested security controls.

CyphiDs will be designed to be run from within a OCI-compatible Linux container for ease of use and portability. Deliverables will include the container configuration and all files necessary to run the CyphiD on both the T&E cyber testbed and on a non-simulated network. Performers are expected to demonstrate their capabilities on the cyber testbed on a non-simulated network. Final deliverable for each CyphiD and APhiD will include the full software development package including any source code, containers, working binary executable, test suite, and documentation. Binaries for each CyphiD will be shared with other Performers during Phase 3 and used as part of ReSCIND prize competition.

1.J. Meeting and Travel Requirements

All Performer teams are expected to attend workshops, technical meetings and other designated meetings to include key personnel from prime and subcontractor organizations.

The ReSCIND program intends to hold a program Kick-off Meeting workshop in the first month of the program and first month of each subsequent program phase. In addition, the program will hold PI Review Meetings (three in Phase 1, two in Phase2, and two in Phase 3). Meetings may be combined for logistical convenience. The dates and locations of these meetings are to be specified at a later date by the Government, but for planning purposes, Offerors should use the approximate times listed in *Table 6* and assume half the PI and kick-off meetings will be on the East Coast (e.g., D.C. area) and half on the West Coast (e.g., San Diego, CA area). IARPA may opt to co-locate the meeting with a relevant external conference or workshop to increase synergy with stakeholders. IARPA reserves the right to change meeting locations and conduct additional site visits on an as-needed basis or virtually, if desired.

Kick-off Meetings will typically be one day in duration and will focus on plans for the coming Phase, Performer planned research, and internal program discussions. PI Review Meetings will typically be two days in duration and will have a greater focus on communicating program progress

and plans to USG stakeholders. These meetings will include additional time allocated to presentation and discussion of research accomplishments.

In both cases, the workshops will focus on technical aspects of the program and on facilitating open technical exchanges, interaction, and sharing among the various program participants. Program participants will be expected to present the technical status and progress of their projects to other participants and invited guests. Individual sessions for each Performer team with the ReSCIND PM and T&E Team may be scheduled to coincide with these workshops. Non-proprietary information will be shared by Performers in the open meeting sessions; proprietary information sharing shall occur during individual breakout sessions with the ReSCIND PM and T&E.

Site visits by the Government Team will generally take place semiannually during each phase. These visits will occur at the Performer's facility. Reports on technical progress, details of successes and issues, contributions to the program goals, and technology demonstrations will be expected at such site visits. IARPA reserves the right to conduct additional site visits on an as-needed basis.

1.K. Glossary of Terms

The following table describes key terms and their definitions in the context of the ReSCIND program.

Table 7: Summary of Key Terms

TERM	Definition in the Context of the ReSCIND Program
Advanced Persistent Threat (APT)	A prolonged and targeted cyberattack using continuous, clandestine, and sophisticated hacking techniques to gain access to a network and remain undetected for an extended period of time, with potentially destructive consequences.
Adaptive Psychology-informed Defense (APhiD)	An AI-guided combination of logic and CyphiDs that dynamically responds to attacker behavior and attributes with a tailored defensive strategy to mitigate attacker success by imposing a cyber penalty.
Attacker Attributes	Behavioral, cognitive, and demographic characteristics of an adversarial human actor (including but not limited to motivation, experience, individual and cultural differences, solitary vs team activity, emotional state, or targeted vs. opportunistic activity) which can be observed with cyber data and exploited for cyber-defensive purposes.
Bias Sensor	Measure of cognitive vulnerability that can be exploited to mitigate attacker success using data available to cyber defenders.
Bias Trigger	Network or host manipulations or other interactions that induce a cognitive vulnerability on a cyber attacker.
Cognitive Biases	Subconscious,[10] systematic errors in thinking that cause misinterpretation of information or deviations from rationality.

[10] Tversky, A. & Kahneman, D. (1974). Judgment under uncertainty: Heuristics and biases, Science, Vol 185(4157), 1124-1131.

TERM	Definition in the Context of the ReSCIND Program
Cognitive Vulnerabilities (CogVulns)	An umbrella term encompassing cognitive and decision-making biases, innate cognitive limitations, emotional or mental state, or physiological vulnerabilities that can result in reduced cyber attacker success or effectiveness.
Cognitive Vulnerability Cluster[11]	A group of related CogVulns that are related, co-occur, manifest behaviorally, or incite a similar cyber behavioral impact.
Cognitive Vulnerability (CogVuln) Playbook	A non-interactive structural representation displaying both hypothesized and confirmed relationships between CogVulns and other relevant variables including how CogVulns, bias triggers, and CyphiDs relate to relevant features including but not limited to: attacker attributes, situational attributes, network and host characteristics, attack phases and TTPs, CogVuln-specific factors (i.e., impact of ambiguity) and cyber behavioral impacts.
Cyber Behavioral Impact	ReSCIND includes seven defender goals that the program will help achieve; these are 1) decrease rate of attack success; 2) increase time to task completion; 3) decrease progress toward goal; 4) decrease time until detection; 5) increase detectability of attacker; 6) increase attacker cognitive effort spent; 7) increase attack resources wasted.
Cyber Operators	The humans performing cyber operations, both defensive (e.g., Incident Response Team, Blue Team, security operations center, Cyber Protection Team) and offensive (e.g., unauthorized/illegal hacker, advanced persistent threat (APT), ethical/legal hacker, Red Team).
Cyberpsychology	The scientific field that integrates human behavior and decision-making into the cyber domain, allowing us to understand, anticipate and influence cyber operator behavior.
Cyber Penalty	Costs (e.g., wasted time, wasted resources) imposed on a cyber attacker designed to mitigate success, using techniques including but not limited to denial, delay, degradation, detection, disruption, or deception.
Cyberpsychology-informed Defense (CyphiD)	A combination of bias sensors, logic, and bias triggers which generates a novel defensive strategy to mitigate attacker success by imposing a cyber penalty.
Human Limitations	Behavioral, social, cultural, physiological or other patterns that are potentially exploitable via cyber operations.
Situational Attributes	Cyber-relevant details about the goals, constraints (i.e., time factors), and characteristics of the cyber situation in question, in which both attacker and defender attributes are considered.
Network and Host Characteristics	Characteristics of hardware and systems architecture (including but not limited to network typology, system appearance, security posture, time delays) which can be exploited for cyber-defensive purposes. These can include factors such as the topology of the network, the types of devices and protocols used, the physical layout

[11] https://www.mitre.org/sites/default/files/publications/pr-16-0956-the-assessment-of-biases-in-cognition.pdf

TERM	Definition in the Context of the ReSCIND Program
	of the network, and the external factors that can affect network performance, such as interference and network traffic.
Security Operations Center (SOC)	A team of cyber experts that monitors and organization's information technology infrastructure 24/7 to detect cybersecurity events in real time and address them as quickly and effectively as possible. ReSCIND solutions should aim to augment an existing SOC, or function where no SOC is available.

2. AWARD INFORMATION:

Research conducted under this project is considered "fundamental research" as defined in 22 C.F.R. § 120.11(8) and 15 C.F.R. § 734.8(c).

The BAA shall result in awards for all Phases of the program. Exercise of the Option Periods shall depend upon performance during Phase I - Base Period and subsequent Option Periods, as well as program goals, the availability of funding, and IARPA priorities. Exercising of Phases II – Option Period 1 and Phase III-Option Period 2 is at the sole discretion of the Government.

Multiple awards are anticipated. Financial resources made available under this BAA shall depend on the quality of the proposals received and the availability of funds. Multiple awards to the same Offeror are acceptable provided the proposed techniques are distinct and the proposed personnel are sufficiently different to achieve the necessary level of effort to complete the work.

The Government reserves the right to select for negotiation all, some, one, or none of the proposals received in response to this solicitation and to make awards without discussions with Offerors. The Government also reserves the right to conduct discussions if determined to be necessary. Additionally, the Government reserves the right to accept proposals in their entirety or to select only portions of proposals for negotiations for award. Evaluation and award of proposals will follow FAR 35 processes as described herein.

Awards under this BAA shall be made to Offerors based on the Evaluation Factors listed in Section 5 of the BAA, as well as successful completion of negotiations. Proposals selected for negotiation may only result in a procurement contract.

The Government shall contact Offerors whose proposals are selected for negotiations to obtain additional information required for award. The Government may establish a deadline for the close of fact-finding and negotiations that allows a reasonable time for the award of a contract. Offerors that are not responsive to Government deadlines established and communicated with the request may be removed from award consideration. Offerors may also be removed from award consideration should the parties fail to reach agreement within a reasonable time on contract terms, conditions, and cost/price.

3. ELIGIBILITY INFORMATION:

3.A. Eligible Applicants

All responsible sources capable of satisfying the Government's needs may submit a proposal. Historically Black Colleges and Universities, Small Businesses, Small Disadvantaged Businesses and Minority Institutions are encouraged to submit proposals and team with others to submit proposals; however, no portion of this announcement shall be set aside for these organizations' participation due to the impracticality of reserving discrete or severable areas for exclusive competition among these entities. Other Government Agencies, Federally Funded Research and Development Centers, University Affiliated Research Centers, Government-Owned, Contractor-

Operated facilities, Government Military Academies, and any other similar type of organization[12] that has a special relationship with the Government, that gives them access to privileged and/or proprietary information or access to Government equipment or real property, are not eligible to submit proposals under this BAA or participate as team members under proposals submitted by eligible entities. An entity of which only a portion has been designated as a UARC may be eligible to submit a proposal or participate as a team member subject to an organizational conflict of interest review.

Foreign entities and/or individuals may propose, even as the prime contractor. However, all foreign participation must comply with any necessary Non-Disclosure Agreements, Security Regulations, Export Control Laws, and other governing statutes applicable under the circumstances. Offerors are expected to ensure that participants do not either directly or indirectly compromise the laws of the United States, nor its security interests. As such, both foreign and domestic Offerors should carefully consider the roles and responsibilities of foreign participants as they pursue teaming arrangements.

3.A.1 Organizational Conflicts of Interest (OCI)

According to FAR 2.101 "Organizational Conflict of Interest" means that because of other activities or relationships with other persons, a person is unable or potentially unable to render impartial assistance or advice to the Government, or the person's objectivity in performing the contract work is or might be otherwise impaired, or a person has an unfair competitive advantage.

In accordance with FAR 9.5, Offerors are required to identify and disclose all facts relevant to potential OCIs involving the Offeror's organization and any proposed team member (sub awardee, consultant). Under this Section, the Offeror is responsible for providing this disclosure with each proposal submitted pursuant to the BAA. The disclosure must include the Offeror's, and as applicable, proposed team member's OCI mitigation plan. The OCI mitigation plan must include a description of the actions the Offeror has taken, or intends to take, to prevent the existence of conflicting roles that might bias the Offeror's judgment and to prevent the Offeror from having an unfair competitive advantage. The OCI mitigation plan will specifically discuss the disclosed OCI in the context of each of the OCI limitations outlined in FAR 9.505-1 through FAR 9.505-4.

IARPA generally prohibits contractors/Performers from concurrently providing Scientific Engineering Technical Assistance (SETA), Advisory and Assistance Services (A&AS) or similar support services and being a technical Performer. Therefore, as part of the FAR 9.5 disclosure requirement above, address whether an Offeror or an Offeror's team member (e.g., sub awardee, consultant) is providing SETA, A&AS, or similar support (e.g., T&E services) to IARPA under: (a) a current award or subaward; or (b) a past award or subaward.

[12] There are instances when these types of entities provide a unique facility, specialized equipment or technical service that is not otherwise obtainable. In such cases, Offerors can request use and the Government will determine if the resource can be made available to all Offerors as Government Furnished Property / Equipment/Information / / Capability / Service. If the resource requested cannot be provided directly by the Government, the Government may consider an Offeror's request for limited use as a procured service not otherwise available only after an OCI review and determination. It is advised that the Offeror have an alternate plan in its proposal in case the Government does not accept the proposed participation. Requests for such resources can be submitted during the Q&A period.

If SETA, A&AS, or similar support is or was being provided to IARPA, the proposal must include:

- The name of the IARPA program or office receiving the support;
- The prime contract number.
- Identification of proposed team member (sub awardee, consultant) providing the support.

As part of their proposal, Offerors shall include either (a) a copy of their OCI notification including mitigation plan or (b) a written certification that neither they nor their subcontractor teammates have any potential conflicts of interest, real or perceived. A sample certification is provided in Appendix A.

The Government will evaluate OCIs and potential OCIs to determine whether they can be avoided, neutralized, or mitigated and/or whether it is in the Government's interest to grant a waiver. The Government will make OCI determinations, as applicable, for proposals that are otherwise selectable under the BAA Evaluation Factors.

The Government may require Offerors to provide additional information to assist the Government in evaluating OCIs and OCI mitigation plans. If a prospective Offeror believes that any conflict of interest exists or may exist (whether organizational or otherwise), the Offeror should promptly raise the issue with the Government by sending his/her contact information and a summary of the potential conflict by e-mail to the Agency Contact identified herein, before time and effort are expended in preparing a proposal and mitigation plan.

If the Government determines that an Offeror failed to fully disclose an OCI; or failed to provide the affirmation of IARPA support as described above; or failed to reasonably provide additional information requested by Government to assist in evaluating the Offeror's OCI and proposed OCI mitigation plan, the Government may reject the proposal and withdraw it from consideration for award.

3.A.2 Multiple Submissions to the BAA

Organizations may participate as a prime or subcontractor in more than one submission to the BAA. However, if multiple submissions to the BAA which include a common team member are selected, such common team members shall not receive duplicative funding (i.e., no one entity can be paid twice to perform the same task).

3.B. U.S. Academic Institutions

According to Executive Order 12333, as amended, paragraph 2.7, "Elements of the Intelligence Community are authorized to enter into contracts or arrangements for the provision of goods or services with private companies or institutions in the United States and need not reveal the sponsorship of such contracts or arrangements for authorized intelligence purposes. Contracts or arrangements with academic institutions may be undertaken only with the consent of appropriate officials of the institution."

Offerors must submit a completed and signed Academic Institution Acknowledgement Letter for each U.S. academic institution that is a part of their team, whether the academic institution is

serving in the role of a prime, or a subcontractor or a consultant at any tier of their team with their technical proposal. Each Letter must be signed by a senior official from the institution (e.g., President, Chancellor, Provost, or other appropriately designated official). A template of the Academic Institution Acknowledgment Letter is enclosed in APPENDIX A of this BAA. Note that the Government shall not enter into negotiations with an Offeror whose team includes a U.S. academic institution until all required Academic Institution Acknowledgment Letters are received.

3.C. Other Eligibility Criteria

3.C.1 Collaboration Efforts

Collaborative efforts and teaming arrangements among potential Offerors are strongly encouraged. Specific content, communications, networking, and team formations are the sole responsibility of the participants.

4. APPLICATION AND SUBMISSION INFORMATION:

This notice constitutes the total BAA and contains all information required to submit a proposal. No additional forms, kits, or other materials are required.

4.A. Proposal Information

Interested Offerors are required to submit full proposals (Volume I, initially and Volume 2, if requested) in order to receive consideration for the award. Compliant proposals shall be received by the time and date specified in the BAA Proposal Due Date for Initial Round of Selections, in order to be considered in the initial round. It is within the Government's sole discretion whether to evaluate any proposals received after this date. Selection for award remains contingent on the technical and funding availability evaluation factors. Proposals received after the BAA Closing Date are deemed to be late and will not be evaluated.

The Government intends to use Booz Allen Hamilton, Whitney, Bradley & Brown, Inc. (WBB), Serco, Inc., Airlin Technologies, Bluemont Technology & Research, Navstar, Crimson Phoenix, Northwood Global Solutions, Onts & Quants, Inc., Tarragon Solutions, and SiteWorks LLC regarding portions of the proposals submitted to the Government and/or to provide logistical support in carrying out the evaluation process.

In addition to supporting evaluations, the following entities: the Naval Information Warfare Center (NIWC) (San Diego, CA), U.S. Army DEVCOM C5ISR Center (Adelphi, MD), Lawrence Livermore National Laboratory (Livermore, CA), and the Massachusetts Institute of Technology - Lincoln Laboratory (MIT-LL) (Lexington, MA), Applied Research Laboratory for Intelligence and Security (ARLIS) (College Park, MD), and MITRE Corporation (Bedford, Massachusetts), may be supporting T&E activities or consulting for contracts awarded under this program and should also be considered as part of an Offeror's OCI disclosure.

All Government and Contractor personnel shall have signed and be subject to the terms and conditions of non-disclosure agreements. By submission of its proposal, an Offeror agrees that its proposal information may be disclosed to employees of these organizations for the limited purposes stated above. Offerors who object to this arrangement shall provide clear notice of their

objection as part of their transmittal letter. If Offerors do not send notice of objection to this arrangement in their transmittal letter, then the Government shall assume consent to the use of contractor support personnel in assisting the review of submittal(s) under this BAA.

Only Government personnel will evaluate and make award determinations under this BAA.

All administrative correspondence and questions regarding this solicitation shall be directed by email to dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov. Proposals shall be submitted in accordance with the procedures stated in the BAA.

4.B. Proposal Format and Content

To facilitate the evaluation of the proposal, the government encourages the Offerors to submit proposals which: are clear and concise; limited to essential matters sufficient to demonstrate a complete understanding of the Government's requirements; include sufficient detail for effective evaluation; and provide convincing rationale to address how the Offeror intends to meet these requirements and objectives, rather than simply rephrasing or restating the Government's requirements and objectives.

All proposals shall be in the format given below. Non-compliant proposals may be rejected without review. Proposals shall consist of "Volume 1 - Technical and Management Proposal" and, only if requested (see BAA sections 4.B.2 and 5.B.), "Volume 2 - Cost Proposal." All proposals shall be written in English.

Additionally, text should be black and paper size 8-1/2 by 12-inch, white in color with 1" margins from paper edge to text or graphic on all sides. The Government desires Times New Roman font with font size not smaller than 12 point. The Government desires that the font size for figures, tables and charts not be smaller than 10 point. All contents shall be clearly legible with the unaided eye. Excessive use of small font, for other than figures, tables, and charts, or unnecessary use of figures, tables, and charts to present information may render the proposal non-compliant. Text and graphics, if applicable, may be printed on both sides of a sheet (double-sided). Front and backside of a single sheet are counted as two (2) pages if both sides are printed upon. Foldout pages are not permitted. The page limitation for full proposals includes all figures, tables, and charts. All pages should be numbered. No other materials may be incorporated in any portion of the proposal by reference, as a means to circumvent page count limitations. All information pertaining to a volume shall be contained within that volume. Any information beyond the page limitations will not be considered in the evaluation of Offerors.

The Government anticipates proposals submitted under this BAA will be UNCLASSIFIED. Proposals shall not contain any classified information.

Each proposal submitted in response to this BAA shall consist of the following:

Volume 1 – Technical & Management Proposal (See Section 4.B.1 below for page limit)

Section 1 – Cover Sheet (see Appendix A) & Transmittal Letter (not included in page count)
Section 2 – Summary of Proposal
Section 3 – Detailed Proposal

Section 4 – Attachments (Not included in page count, but number appropriately for elements included. Templates are in the Appendices of this BAA).

1 – Academic Institution Acknowledgment Letter, if required

2 – IP Rights, estimated not to exceed 4 pages

3 – OCI Notification or Certification

4 – Bibliography

5 – Relevant Papers (up to three)

6 – Consultant Letters of Commitment

7 – Human Use Documentation (see Section ~~6.B.9.~~ 6.B.8. For informational purposes, acknowledge and submit requirements through Appendix A.7)

8 – Animal Use Documentation - **Not applicable**

9 – A Three Chart Summary of the Proposal

10 – Security Plan - **Not applicable**

11 – Research Data Management Plan (RDMP), not to exceed 3 pages (see Section 4 and Template under Appendix A)

12 – Privacy Plan, not to exceed 4 pages

13 – Experimental Protocol (See Appendix A.7), maximum 18 pages, not including standard questionnaires and inventories. Submissions shall not contain any proprietary information. This attachment shall be uploaded as a separate document from the Technical Proposal at the time of submission.

Volume 2 – Cost Proposal
(To be submitted only upon request of the Contracting Officer, See BAA Sections 4.B.2 and 5.B)

Section 1 – Cover Sheet (see Appendix B)

Section 2 – Estimated Cost Breakdown

Section 3 – Supporting Information

4.B.1 Volume 1: Technical and Management Proposal

Volume 1, Technical and Management Proposal, may include an attached bibliography of relevant technical papers or research notes (published and unpublished) which document the technical ideas and approach on which the proposal is based. Copies of not more than three relevant papers can be included with the submission. Other supporting materials will not be reviewed. For purposes of page limit determination only, Offerors must propose to all three phases. Except for the cover sheet, transmittal letter, table of contents (optional), and the required attachments stated in the BAA the allowable page limits are as follows:

- **Not to exceed 30 pages**

Any pages exceeding these limits will not be considered during the evaluation process. Proposals shall be accompanied by an official transmittal letter, using contractor format.

4.B.1.a Section 1: Cover Sheet & Transmittal Letter

A. Cover sheet: (See Appendix A for template)

B. Transmittal Letter

The transmittal letter shall include the following **(not to exceed one page)**:

Introduction of Offeror and team (subcontractors and consultants), the BAA number, IARPA program name, Offerors' Program name, the proposal validity period, the type contract vehicle being requested (procurement contract or other transaction) with a short rationale, any non-negotiable conditions on which the offer is based such as contract type (cost type, FFP), IP restrictions, etc., and the Offeror's points of contact information including: name, email and phone number for both technical and administrative issues.

Note: Any information required elsewhere in the proposal must be included in the appropriate section of the proposal (i.e., including the information in the transmittal letter alone may not be sufficient). If there is a conflict between the transmittal letter and the proposal the proposal shall control.

4.B.1.b Section 2: Summary of Proposal (see below for page limit)

Section 2 shall provide an overview of the proposed work as well as introduce associated technical and management issues. This section shall contain a technical description of technical approach to the research as well as a succinct portrayal of the uniqueness and benefits of the proposed work. It shall make the technical objectives clear and quantifiable and shall provide a project schedule with definite decision points and endpoints.

- **Not to exceed 5 pages**

The Summary shall include the elements specified in the sections below:

A. A technical overview of the proposed research and plan. This section is the centerpiece of the proposal and shall succinctly describe the proposed approach and research. The overview shall clearly articulate the approach and design, technical rationale, and constructive plan for accomplishment of technical objectives and deliverable production. The approach will be supported by basic, clear calculations. Additionally, proposals shall clearly explain the innovative claims and technical approaches that will be employed to meet or exceed each program metric along with an explanation outlining why the proposed approaches are feasible. Proposals must also clearly identify any technical uncertainties and potential mitigations. The use of non-standard terms and acronyms should be avoided. This section shall be supplemented with a more detailed plan in Volume 1, Section 3 of the proposal.

B. Summary of the products, transferable technology and deliverables associated with the proposed research results. Define measurable deliverables that show progress toward achieving the stated program milestones. All proprietary claims to the results, prototypes, IP, or systems supporting and/or necessary for the use of the research, results, and/or prototype

shall be detailed in Attachment 2. Should no proprietary claims be identified in Attachment 2, Government rights shall be unlimited to all technology and deliverables resulting from or delivered under this BAA.

C. Schedule and milestones for the proposed research. Summarize, in table form the schedule and milestones for the proposed research. Do not include proprietary information with the milestone chart.

D. Related research. Include a general discussion of other research in this area, comparing the significance and plausibility of the proposed innovations against competitive approaches to achieve Program objectives.

E. Project contributors. Include a clearly defined organizational chart of all anticipated project participants and affiliations (e.g. subcontractor, consultant), organized under functional roles for the effort, along with the associated task number responsibilities for each individual.

F. Technical Resource Summary: **(NOTE: The full Cost Volume is not required unless requested by the Contracting Officer; therefore, it is critical that Offerors address the items below in their technical proposal so the Government can evaluate Resource Realism.)**

- Summarize the total level of effort by labor category/technical discipline (e.g., research scientist/chemist/physicist/engineer/administrative) and affiliation (e.g., prime/ subcontractor/consultant). All Key Personnel and significant contributors shall be identified by name. Provide a brief description of the qualifications for each labor category/technical discipline (e.g., education, certifications, years of experience).
- Summarize level of effort by labor category/technical discipline for each major task.
- Identify software and IP required for performance, by affiliation. List each item separately, identifying the task number for which the software or IP is required and the Performer team requiring it.
- Identify materials or equipment (such as IT) required for performance. List each item separately, identifying the task number for which the material or equipment is required and the Performer team requiring it.
- Identify any other resources required to perform (e.g., services, data sets, data set repository, facilities, Government furnished property. List each item separately, identifying the task number for these other resources are required and the Performer team requiring it.
- Estimated travel, including purpose of travel and number of personnel per trip, by affiliation. (See Appendix B.4 for sample template)

The above information shall cross reference to the tasks set forth in the Offeror's statement of work and shall be supported by the detailed cost and pricing information provided in the Offeror's Volume 2 Cost Proposal, the latter of which shall be submitted only if requested.

4.B.1.c. Section 3: Detailed Proposal Information

This section of the proposal shall provide the detailed, in-depth discussion of the proposed research as well as supporting information about the Offeror's capabilities and resources. Specific attention

shall be given to addressing both the risks and payoffs of the proposed research and why the proposed research will achieve the goals, objectives, metrics, and milestones in this BAA. The Government reserves the right to reject a proposal if the information requested below is not adequately addressed. This part shall provide:

A. Statement of Work (SOW) (See Appendix A for Sample Format) - Clearly define the technical tasks and sub-tasks to be performed, their durations and the dependencies among them. For each task and sub-task, provide:

- A general description of the objective;
- A detailed description of the approach to be taken, developed in an orderly progression and in enough detail to establish the feasibility of accomplishing the goals of the task;
- Identification of the primary organization responsible for task execution (prime, sub-contractor, team member, etc.) by name;
- The exit criteria for each task/activity (i.e., a product, event or milestone that defines its completion); and
- Definition of all deliverables (e.g., data rights, reports, software) to be provided to the Government.

Note: Do not include any proprietary information in the SOW

At the end of this section of the proposal, provide a Gantt chart, showing all the tasks and sub-tasks on the left (grouped by technical challenge) with the performance period (in years/quarters) on the right. All milestones shall be clearly labeled on the chart. If necessary, use multiple pages to ensure legibility of all information.

B. A detailed description of the objectives, scientific relevance, technical approach and expected significance of the work. Clearly identify the key elements of the proposed work and how they relate to each other. Describe the technical methods or approaches that will be used to meet or exceed each program milestone along with an explanation outlining why the proposed methods/approaches are feasible. Additionally, describe any anticipated risks along with possible mitigations. Proposals containing only a general discussion of the problem without detailed description of approaches, plausibility of implementation, and critical metrics may be deemed not selectable.

C. State-of-the-art. Compare with the proposed approach to other on-going research, highlighting the uniqueness of the proposed approach and differences between the proposed effort and the current state-of-the-art. Identify advantages and disadvantages of the proposed work with respect to potential alternative approaches.

D. Data sources. Identify and describe data sources to be utilized in pursuit of the stated research goals.

Offerors proposing to use existing data sets shall provide written verification that said data sets were obtained in accordance with U.S. laws and, where applicable, use will be in compliance with End User License Agreements, Copyright Laws, Terms of Service, and laws and policies regarding privacy protection of U.S. Persons. Offerors proposing to obtain new data sets shall ensure that their plan for obtaining the data complies with U.S. Laws and, where applicable, with End User License Agreement, Copyright Laws, Terms

of Service, and laws and policies regarding privacy protection of U.S. Persons. Offerors shall also address IP restrictions on the use or transfer of such data sets, in Attachment 2 of the Offeror's proposal, as described in Section 4.B.1.d.

Offerors shall also include the documentation required in 6.B. (Human Use).

Documentation must be well written and logical; claims for exemptions from Federal regulations for human subject protection must be accompanied by a strong defense of the claims. The Human Use documentation and the written verification are not included in the total page count.

E. Deliverables. Based on the required deliverables identified in Section 1 of the BAA, clearly identify the hardware and data to be delivered, including technical data and computer software. In Attachment 2 to Offeror's proposal, Offerors shall address IP rights in such data, as described in Section 4.B.1.d.

F. Cost, schedule, milestones. Describe the cost, schedule, and milestones for the proposed research, including cost estimates by cost element for base period, the option period(s) and the total program summary, and company cost share, if any, ~~as well as, costs by technical area(s)~~ and tasks (see tables below for sample format). The milestones shall not include proprietary information (Offeror can use their own format for milestones).

(Note: The full Volume 2 - Cost Proposal is not required unless requested by the CO; therefore, it is critical that Offerors address this element in their technical proposal so the Government can evaluate funding availability. See BAA Sections 4.B.2, 5.A., and 5.B).

SAMPLE FORMAT

Cost Element (burdened)	**Phase 1- Base (18 Months)**	**Phase 2 - Option 1 (~~12~~ 15 Months)**	**Phase 3 – Option 2 (12 Months)**	**Total Program Summary**
Labor				
Subcontracts/Consultant				
Materials & Equipment				
Travel				
Other Direct Costs				
(Cost Share, if any)				
Total				

G. Offeror's previous accomplishments. Discuss previous accomplishments and work in this or closely related research areas and how these will contribute to and influence the current work.

H. Facilities. Describe the facilities that shall be used for the proposed effort, including computational and experimental resources.

I. Detailed Management Plan. Provide the Management Plan that clearly identifies both organizations and individuals within organizations that make up the team, and delineate

the expected duties, relevant capabilities, and task responsibilities of team members and expected relationships among team members. Identify the expected levels of effort (percentage time, or fraction of an FTE) for all Key Personnel and significant contributors. Additionally, include a description of the technical, administrative, and business structure of the team along with an internal communications plan. Describe project/function/sub-contractor relationships (including formal teaming agreements), Government research interfaces, and planning, scheduling, and control practices utilized, as well as the team leadership structure. Provide a brief biography of all Key Personnel (including alternates, if desired) and significant contributors who shall be involved in the research along with the amount of effort to be expended by each person during the year. Participation by all Key Personnel and significant contributors is expected to exceed 25% of their time. A compelling explanation is required for any variation from this figure.

If the team intends to use consultants, they shall also be included in the organizational chart with an indication of whether the person shall be an "individual" or "organizational" consultant (i.e., representing themselves or their organization), and organizational affiliation.

See Table 4 below for the recommended format.

Table 4: Team Organization (Example) * if applicable

Participants	Org	Role	Unique, Relevant	Role: Tasks	Clearance Level *	Time
Jane Wake	LMN Univ.	PI/Key Personnel	Electrical Engineering	Program Mgr & Electronics: 10		100%
John Weck, Jr.	OPQ Univ.	Key Personnel	Mathematical Physics	Programming: 1-5		50%
Dan Wind	RST Univ.	Key Personnel	Physics	Design, Fab, and Integration: 6-8		90%
Katie Wool	UVW Univ.	Contributor	Quantum Physics	Enhancement witness design: 4		25%
Rachel Wade	XYZ Corp.	Co-PI/Key Personnel	Graph theory	Architecture design: 6		55%
Chris West	XYZ Corp.	Significant Contributor	EE & Signal Processing	Implementation & Testing: 8-9		60%
Julie Will	JW Cons.	Consultant (Individual)	Computer science	Interface design: 10		200 hours
David Word	A Corp.	Consultant (A. Corp.)	Operations Research	Applications Programming: 2-3		200 hours

J. Resource Share. Include the type of support, if any, the Offeror might request from the Government, such as facilities, equipment, materials, or any such resources the Offeror is willing to provide at no additional cost to the Government to support the research effort. Cost sharing is not required from Offerors and is not an evaluation criterion but is encouraged where there is a reasonable probability of a potential commercial application related to the proposed research and development effort.

K. The names of other federal, state, or local agencies or other parties receiving the proposal and/or funding the proposed effort. If none, so state. Concurrent submission of the proposal to other organizations will not prejudice its review but may impact IARPA's decision to fund the effort. See 5.A.2.a.

L. Research Data Management Plan. (RDMP). Submit a RDMP that outlines how they will manage and preserve the Research Data, as defined below, collected, or produced through the course of performance. The RDMP need not require the preservation of all Research Data: Offerors shall consider the cost and benefits of managing and preserving the Research Data in determining whether to preserve it. At a minimum, all Research Data associated with a peer-reviewed manuscript or final published article (hereinafter "Publications") must be made publicly accessible by the award recipient before, on or at a reasonable time after the publication date. The Publications whose associated data must be covered by the RDMP are deliverables as described in Section 1.

Research Data is defined herein as the digital recorded factual material commonly accepted in the scientific community as necessary to validate research findings including data sets used to support scholarly publications, but does not include laboratory notebooks, preliminary analyses, drafts of scientific papers, plans for future research, peer review reports, communications with colleagues, or physical objects, such as laboratory specimens.

The RDMP must address the following:

- Describe the types of Research Data collected or produced in the course of the project. Include standards to be used for Research Data and metadata content and format.
- A plan for making the Research Data that underlie Publications digitally accessible to the public before or, at the time of publication or conference presentation, or within a reasonable time after publication. The requirement could be met by including the data as supplementary information to the Publication or by depositing the Research Data in a searchable, machine-readable, and digitally accessible form suitable for repositories available to the public free of charge. Such repositories could be discipline-specific repositories, general purpose research data repositories or institutional repositories. The published article or conference paper should indicate how the public may access Research Data underlying the paper's results and findings. Offerors should attempt to make the Research Data available for at least three years after published article or conference. (NOTE: Offerors shall make a best effort in identifying research data sets that may be used for Publications that occur after contract end. The Offeror shall deliver these data sets to the Government and make them available in repositories available to the public prior to the end of the period of performance, if not included as supplementary information to Publications.)
- Policies and provisions for sharing and preservation, including a) policies and provisions for appropriate protection of privacy, confidentiality, security, and IP, b) descriptions of tools, including software, needed to access and interpret the Research Data, and c) policies and provisions for re-use, re-distribution, and production of derivatives.

- If, for legitimate reasons (e.g., privacy, confidentiality, security, IP rights considerations; size of data sets, cost; time), the Research Data underlying the results of peer-reviewed publications or conference papers cannot be shared and preserved, the plan must include a justification citing such reasons.

In addressing these elements (e.g., types of data to be shared and preserved, standards to be used for data and metadata, repositories to be used for archiving data, timeframes for sharing and preservation), the RDMP should reflect the best practices of the relevant scientific discipline and research community. At a minimum, Research Data underlying Publications and associated metadata shall include an acknowledgement of IARPA support and a link to the associated Publication.

4.B.1.d. Section 4: Attachments

[NOTE: The attachments listed below shall be included with the proposal, if applicable, but do not count against the Volume 1-page limit.]

Attachment 1: Signed Academic Institution Acknowledgement Letter(s) (if applicable). A template is provided in Appendix A.

Attachment 2: IP Rights. A template is provided in Appendix A. This attachment is estimated not to exceed 4 pages and shall address the following:

Representation as to Rights. An Offeror shall provide a good faith representation that they either own or have sufficient licensing rights to all IP that will be utilized under their proposal.

Program-Specific IP Approach. IARPA requires sufficient rights to IP developed or used in the conduct of the proposed research to ensure that IARPA can successfully (a) manage the program and evaluate the technical output and deliverables, (b) communicate program information across Government organizations, and (c) support transition to and further use and development of the program results by Intelligence community (IC) users and others. IARPA anticipates that achieving these goals for the ReSCIND program will necessitate a minimum of Unlimited Rights in all deliverables. However, there may be any number of other approaches to intellectual property rights to achieve IARPA's program goals. "Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so. In addressing their approach to IP rights, Offerors should (1) describe the intended use of patented invention(s) or data, including, technical data and computer software, in the conduct of the proposed research; (2) describe the rights being offered to the Government along with a justification if less than Unlimited Rights is being offered; (3) explain how IARPA will be able to reach its program goals (including transition) with the rights offered to the Government; (4) identify the cost to the Government to acquire additional or alternative rights beyond those being offered, if applicable; and (5) provide possible alternatives in any area in which the offered rights may be insufficient for IARPA to achieve its program goals (e.g., the possibility of future licensing of privately-developed software to U.S. Government agencies at a reasonable cost.)

Patented Inventions. **Offerors shall include documentation using the format provided in Appendix A,** proving ownership of or sufficient rights to all inventions (or inventions for which a patent application has been filed) that will be utilized under the proposal for the IARPA program. If a patent application has been filed for an invention that the proposal utilizes, but the application has not yet been made publicly available and contains proprietary information, the Offeror may provide only the serial number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and a summary of the patent title, together with either: (1) a representation that the Offeror owns the invention, or (2) proof of sufficient licensing rights in the invention. Offerors shall also indicate their intention to incorporate patented technology into any deliverable- i.e., if Offerors intend for any deliverable to embody any invention covered by any patent or patent application the Offerors listed in Volume 1, Attachment 2, Offerors should also specify in the Attachment the deliverable into which the Offerors expects to incorporate the invention. In doing so, the Government requests that Offerors further specify any rights offered to the Government for inventions that shall be utilized in the program (beyond the implied license that accompanies a patent owner's sale of a patented product).

Noncommercial Data. Offerors shall identify all noncommercial data, including technical data and computer software, that it plans to generate, develop and/or deliver under any proposed award instrument in which the Government shall acquire less than unlimited rights. In doing so, Offerors must assert (a) the specific restrictions the Government's rights in those deliverables, (b) the basis for such restrictions, (c) the intended use of the technical data and noncommercial computer software in the conduct of the proposed research and development of applicable deliverables, and (d) a supporting rationale of why the proposed approach to data rights is in the Government's best interest (please see program specific goals above). **If no restrictions are intended, then the Offeror shall state "NONE."**

Commercial Data. Offerors shall identify all commercial data, including technical data and commercial computer software, that may be included in any deliverables contemplated under the research effort and assert any applicable restrictions on the Government's use of such commercial data (please see program specific goals above). **If no restrictions are intended, then the Proposer shall state "NONE."**

Data Developed with Mixed Funding. If mixed funding is anticipated in data generated, developed, and/or delivered under the research effort, the Government seeks at minimum "Government Purpose Rights" (GPR) for all noncommercial data deliverables; offering anything less shall be considered a weakness in the proposal. United States Government purposes include any activity in which the United States Government is a party, including cooperative agreements with international or multi-national defense organizations, or sales or transfers by the United States Government to foreign governments or international organizations. Government purposes include competitive procurement, but do not include the rights to use, modify, reproduce, release, perform, display, or disclose technical data or computer software for commercial purposes or authorize others to do so. Government Purpose Rights continue for a five-year period upon execution of the contract, and upon expiration of the five-year period, the Government obtains Unlimited Rights in the data.

Open Source. If Offerors propose the use of any open-source data or freeware, any conditions, restrictions, or other requirements imposed by that software shall also be addressed. Offerors should leverage the format in **Appendix A** for their response.

Identification of Relevant Government Contracts. For all technical data and computer software that an Offeror intends to deliver with other than unlimited rights that are identical or substantially similar to technical data and computer software that the Offeror has produced for, delivered to, or is obligated to deliver to the Government under any contract or subcontract, the Offeror shall identify (a) the contract number under which the data, software, or documentation was produced; (b) the contract number under which, and the name and address of the organization to whom, the data and software was most recently delivered or shall be delivered; and (c) any limitations on the Government's rights to use or disclose the data and software, including, when applicable, identification of the earliest date the limitations expire.

Definitions. For this solicitation, the Government recognizes only the definitions of IP rights in accordance with the terms as set forth in the Federal Acquisition Regulation (FAR) part 27, Defense Federal Acquisition Regulation Supplement (DFARS) part 227, or as defined herein. If Offerors propose IP rights that are not defined in FAR part 27, DFARS part 227, or herein, Offerors shall clearly define such rights in the "Intellectual Property Rights" Attachment of their proposal. Offerors are reminded of the requirement for prime contractors to acquire sufficient rights from subcontractors to accomplish the program goals.

Evaluation. The Government may use the asserted data rights during the evaluation process to evaluate the impact of any identified restrictions. The technical content of the "Intellectual Property Rights" Attachment shall include only the information necessary to address the proposed approach to IP; any other technical discussion in the attachment shall not be considered during the evaluation process.

Attachment 3: OCI Notification or Certification Template provided in Appendix A.

Attachment 4: Bibliography. A brief bibliography of relevant technical papers and research notes (published and unpublished) which document the technical ideas on which the proposal is based.

Attachment 5: Relevant Papers. Copies of not more than three relevant papers may be included in the submission. The Offerors shall include a one-page technical summary of each paper provided, suitable for individuals who are not experts in the field.

Attachment 6: Consultant Commitment Letters. If needed.

Attachment 7: Human Use Documentation, reference section 6.B.9.

Attachment 8: Animal Use Documentation. **Not applicable**

Attachment 9: A Three Chart Summary of the Proposal. A PowerPoint summary that quickly and succinctly indicates the concept overview, key innovations, expected impact, and other unique aspects of the proposal. The format for the summary slides is included in Appendix A to this BAA and does not count against the page limit. Slide 1 should be a self-contained, intuitive description of the technical approach and performance. These slides may be used during the evaluation process to present a summary of the proposal from the Offeror's view.

Attachment 10: Security Plan. **Not applicable**

Attachment 11: RDMP (estimated as 2 to 3 pages). Template provided in Appendix A.

Attachment 12: Privacy Plan, (4-page limit). As part of their proposal, Offeror's shall prepare a ReSCIND Privacy Plan v1.0 that comprehensively describes the efforts the Offeror will take to protect personally identifiable information and safeguard the security of any personal data collected and that of any devices, applications, networks, or services involved in collection, transmission, processing, and storage of such data. Any claims that data are anonymous must be based on evidence and supported with sufficient information regarding how the data have been anonymized.

The initial version of the ReSCIND Privacy Plan shall be included in the Offeror's proposal as a standalone appendix. The ReSCIND Privacy Plan shall be updated at the beginning of each Phase and whenever new sources of data or datasets are proposed for use within a Performer's ReSCIND research activities, to include data used for either development or evaluation purposes.

Attachment 13: Experimental Protocol: **The sections listed in Appendix A.7 are mandatory**. The Offeror can add other sections as appropriate (maximum 18 pages, not including standard questionnaires and inventories). If the information is included in a different section of the proposal or another attachment, then the Offeror shall summarize and state: "See Section X.X of Technical Proposal" or "See page 2 of Privacy Plan".

4.B.2. Volume 2: Cost Proposal (No Page Limit)

NOTE: This Volume is only required if the Offeror's proposal has been selected for negotiation (see BAA Section 5.B and 5.C). The notification of selection for negotiation will be issued in writing by the Contracting Officer and will include a request to submit the full Cost Volume within 10 business days or as otherwise authorized by the Contracting Officer.

The Government anticipates awarding cost-type procurement contracts however, Offerors requesting anything other than a cost-type procurement contract (i.e., Firm Fixed Price (FFP) contract) may be directed by the Contracting Officer to provide "other than certified cost or pricing data" (reference FAR Part 15.4) and/or cost supporting information in a different format than described below. The Contracting Officer will determine whether to grant the request for other than a cost-type procurement contract. Examples of requests that would be considered for approval include those from non-traditional contractors such as commercial entities that do not accept FAR-based cost contracts, small businesses, start-up companies, consortia that may include universities and non-profits or foreign companies; where cost-sharing or government participation in the work is appropriate; where flexibility not available under a procurement contract is needed; or where commercialization by industry is deemed advantageous to the Government.

Regardless of the type of instrument determined to be appropriate by the CO, the Offeror's cost proposal shall contain sufficient information to establish the Offeror's understanding of the project, the perception of project risks, the ability to organize and perform the work and to support the realism and reasonableness of the proposed cost, to the extent appropriate. The Government recognizes that undue emphasis on cost may motivate Offerors to offer low-risk ideas with minimum uncertainty and to staff the effort with junior personnel to be in a more competitive posture. The Government discourages such cost strategies. Cost reduction approaches that shall

be received favorably include innovative management concepts that maximize direct funding for technology and limit diversion of funds into overhead.

4.B.2.a Section 1: Cover Sheet.

See Appendix B for the Cover Sheet Template

4.B.2.b. Section 2: Estimated Cost Breakdown.

Offerors shall submit numerical cost and pricing data using Microsoft Excel. The Excel document, in the format provided in Appendix B, shall include intact formulas and shall not be hard numbered. The base and option period cost data should roll up into a total cost summary. The Excel files may be write-protected but shall not be password protected. The Cost/Price Volume shall include the following:

A. Completed Cost/Price Template - Offerors shall submit a cost element breakdown for the base period, each option period and the total program summary in the format provided in Appendix B.

B. Total cost broken down by major task.

C. Major program tasks by fiscal year.

D. A summary of projected funding requirements by month.

E. A summary table listing all labor categories used in the proposal and their associated direct labor rates, along with escalation factors used for each base year and option year.

F. A summary table listing all indirect rates used in the proposal for each base year and option year.

4.B.2.c. Section 3: Supporting Information

In addition to the above, supporting cost and pricing information shall be provided in sufficient detail to substantiate the Offeror's cost estimates. Include a description of the basis of estimate (BOE) in a narrative for each cost element and provide supporting documentation, as applicable:

Direct Labor – Provide a complete cost breakout by labor category, hours, and rates (template available in Appendix B). Specify all Key Personnel by name and clearly state their labor category and proposed rate. Describe the basis of the proposed rates and provide a copy of the most recent Forward Pricing Rate Agreement (FPRA) with the Government. If Offerors do not have a current FPRA with the Government, provide payroll records or contingency hire letters with salary data to support each proposed labor category, including those for key individuals, and the most recent Forward Pricing Rate Proposal Submission, if applicable. Offeror should also address whether any portion of their labor rates is attributable to uncompensated overtime.

Labor Escalation Factor – State the proposed escalation rate and the basis for that rate (e.g., based upon Global Insight indices, Cost Index, or historical data). If the escalation rate is based upon historical data, provide data to demonstrate the labor escalation trend. Provide a sample calculation demonstrating application of the factor to direct labor.

Subcontracts (to include consultants and Inter-organizational Transfers (IOTs) – The Offeror is responsible for compiling and providing full subcontractor proposals with the Cost Volume. Subcontractor cost element sheets shall be completed for the base period, each option period and the total summary using the same format required for the prime contractor (See Appendix B). Consultant letter(s) of commitment shall also be attached.

Information shall be presented in Excel with intact formulas using the format provided in Appendix B and addressing the supporting cost information as outlined in Section 4 of the BAA. In addition to the full and complete subcontractor cost proposals, the Offeror shall also provide its analysis of each subcontractor's proposal including justification for why the subcontractor was selected and its determination that the cost/price is fair and reasonable (Reference FAR Part 44 and FAR clause 52.244-2). **If subcontractors have concerns about proprietary cost information, subcontractors may submit their detailed cost proposals directly to the CO.**

Materials and Equipment – Provide copies of quotes, bill of materials, historical data or any other information including Offeror's analysis to support proposed costs.

Travel - The proposed travel supporting detail shall include destination and purpose of the trip, number of trips, number of travelers and days per trip and price per traveler in sufficient detail to verify the BOE. Proposed travel costs shall comply with the limitations set forth in FAR Part 31. (See Appendix B.4 for sample format).

Proposed conference travel must have an immediate, direct, and tangible benefit to the Government such as providing a deliverable at the conference (e.g., gives a presentation, presents a paper or research findings that are sponsored in whole or in part by IARPA). Travel for personnel to simply attend a conference will not be approved as a direct charge to the contract.

Other Direct Costs (ODCs) – ODCs shall be listed separately and supported by quotes, historical data or any other information including the Offeror's analysis.

Indirect Costs – The Offeror shall show indirect cost calculations, identify the proposed indirect rate by contractor fiscal year and program period (base, option period) and provide information on indirect cost pools and allocation bases for each year and program period involved. If a Government agency recently audited the Offeror's indirect rates, the Offeror shall identify the agency that conducted the audit, when the rates were approved and the period for which they are effective. Include a copy of this rate agreement. Absent current Government rate recommendations, it is incumbent on the Offeror to provide some other means of demonstrating indirect rate realism (e.g., 3 years of historical actual costs with applicable pools and bases). If proposed rates vary significantly from historical experience, the Offeror shall explain the variance.

Cost sharing – Describe the source, nature, and amount of cost-sharing, if any. Reference Resource Share from Section 4 of the BAA.

Other Pricing Assumptions – Identify all pricing assumptions, that should be incorporated into the resulting award instrument (e.g., use of Government Furnished Property/Facilities/Information, access to Government Subject Matter Experts, etc.). Reference Resource Share from Section 4 of the BAA.

Facilities Capital Cost of Money (FCCM) – If proposing FCCM, the Offeror shall show FCCM cost calculations, identify the proposed FCCM factors by contractor fiscal year and program year and provide a copy of the Forward Price Rate Agreement (FPRA), Forward Price Rate System (FPRS) or Forward Pricing Rate Recommendation (FPRR), if available.

Profit/Fee - Identify the proposed profit or fee percentage and the proposed profit/fee base. Provide justification for your proposed profit or fee.

Systems - For the systems listed below, provide a brief description of the cognizant federal agency and audit results. If the system has been determined inadequate, provide a short narrative describing the steps your organization has taken to address the inadequacies and the current status. If a formal audit has been performed by a Government Agency, please provide a complete copy of the audit report or adequacy determination letter. If the system has never received a formal Government review and approval include a statement to that effect. Address whether your organization has contracts that are Cost Accounting Standards (CAS) covered and if so, whether they are subject to full or modified CAS coverage.

- Accounting system
- Purchasing system

Certified "cost or pricing data" may be requested for procurement contract awards that exceed the threshold for submittal as set forth in the FAR, unless the Contracting Officer approves an exception from the requirement to submit cost or pricing data. (Reference FAR Part 15.403.)

4.C. Submission Details

4.C.1. Due Dates

See BAA General Information Section for proposal due dates and times.

4.C.2. Proposal Delivery

Proposals (Volume 1 **initially**) shall be submitted electronically through the IARPA Distribution and Evaluation System (IDEAS). Offerors interested in providing a submission in response to this BAA shall first register by electronic means in accordance with the instructions provided on the following web site: https://iarpa-ideas.gov**.** Offerors who plan to submit proposals for evaluation are strongly encouraged to register at least one week prior to the due date for the first round of proposals. Offerors who do not register in advance do so at their own risk, and IARPA shall not extend the due date to accommodate such Offerors. Failure to register as stated shall prevent the Proposer's submittal of documents.

After registration has been approved, Offeror's should upload a proposal, (initially Volume 1 **only**), scanned certifications and permitted additional information in 'pdf' format, or as otherwise directed (Excel, PowerPoint, etc.). Offerors are responsible for ensuring a compliant

and timely submission of their proposals to meet the BAA submittal deadlines. Time management to upload and submit is wholly the responsibility of the Offeror. **Note: IDEAS will require Offerors to complete a proposal cover sheet within IDEAS at the time that the Volume 1 – Technical and Management Proposal is submitted. This is separate and distinct from the Technical and Cost Volume cover sheets referenced in 4.B.1.a. and 4.B.2.a. and provided in Appendices A and B, respectively. Information requested within IDEAS will include basic cost information (Total funds requested from IARPA, proposed costs by option period and validity period). Please complete the requested information, but DO NOT upload your Volume 2 – Cost Proposal. Directions for submittal of Volume 2 – Cost Proposal will be provided by the CO when Offerors are notified of selection for negotiations.**

Upon completing the proposal submission, the Offeror shall receive an automated confirmation email from IDEAS. Please forward that automated message to dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov. IARPA strongly suggests that the Offeror document the submission of their proposal package by printing the electronic receipt (time and date stamped) that appears on the final screen following compliant submission of a proposal to the IDEAS website.

Volume 1 submitted by any means other than IDEAS (e.g., hand-carried, postal service, commercial carrier and email) shall not be considered unless the Offeror attempted electronic submittal but was unsuccessful. Should an Offeror be unable to complete the electronic submittal, the Offeror shall employ the following procedure. The Offeror shall send an e-mail to dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov, prior to the proposal due date and time specified in the BAA and indicate that an attempt was made to submit electronically and that the submittal was unsuccessful. This e-mail shall include contact information for the Offeror. Upon receipt of such notification, the Government will provide additional guidance regarding submission.

Volume 1 shall be submitted by the date and time specified in the BAA, Overview section, Proposal Due Date for Initial Round of Selections, in order to be considered in the initial round. It is in IARPA's sole discretion whether to evaluate proposals received after this due date set forth in the Overview Section. Selection remains contingent on the technical and funding availability evaluation factors. Proposals received after the due date are deemed to be late and will not be reviewed. Failure to comply with the submission procedures may result in the submittal not being evaluated.

Although classified proposals are not anticipated for this program, if an offeror chooses to submit a classified proposal, the offeror must first contact IARPA via dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov for detailed submittal instructions. In no case shall classified information be uploaded into IDEAS.

Classified proposals are not anticipated for this program. In no case shall classified information be uploaded into IDEAS,

4.D. Funding Restrictions

Facility construction costs are not allowable under this activity. Funding may not be used to pay for commercialization of technology.

5. PROPOSAL REVIEW INFORMATION:

5.A. Technical and Funding Availability Evaluation Factors

The factors used to evaluate and select proposals for negotiation for this Program BAA are described in the following paragraphs. Because there is no common SOW, each proposal shall be evaluated on its own merits and its relevance to the Program goals rather than against other proposals submitted in response to this BAA. The proposals shall be evaluated based on technical and funding availability factors. These are of equal importance. Within the technical evaluation factor, the specific technical criteria are in descending order of importance, as follows: Overall Scientific and Technical Merit, Effectiveness of Proposed Work Plan, Contribution and Relevance to the IARPA Mission and Program Goal, Relevant Experience and Expertise, and Resource Realism. Specifics about the evaluation criteria are provided below.

Award(s) shall be made to an Offeror based on the technical and funding availability factors listed below, and subject to successful negotiations with the Government. Award shall not be made to Offeror(s) whose proposal(s) are determined not to be selectable. Offerors are cautioned that failure to follow submittal instructions may negatively impact their proposal evaluation or may result in rejection of the proposal for non-compliance.

5.A.1. Technical Evaluation Factor (technical criteria listed below)

5.A.1.a. Overall Scientific and Technical Merit

Overall scientific and technical merit of the proposal is substantiated, including unique and innovative methods, approaches, and/or concepts. The Offeror clearly articulates an understanding of the problem to be solved. The technical approach is credible and includes a clear assessment of primary risks and a means to address them. The proposed research advances the state-of-the-art.

5.A.1.b. Effectiveness of Proposed Work Plan

The feasibility and likelihood that the proposed approach will satisfy the Program's milestones and metrics are explicitly described and clearly substantiated along with risk mitigation strategies for achieving stated milestones and metrics. The proposal reflects a mature and quantitative understanding of the program milestones and metrics, and the statistical confidence with which they may be measured. Any Offeror proposed milestones and metrics are clear and well-defined, with a logical connection to enabling Offeror decisions and/or Government decisions. The schedule to achieve the milestones is realistic and reasonable.

The roles and relationships of prime and sub-contractors are clearly delineated with all participants fully documented. Work plans shall demonstrate the ability to provide full Government visibility into and interaction with key technical activities and personnel, and a single point of responsibility for contract performance. Work plans shall also demonstrate that all Key Personnel and significant

contributors have sufficient time committed to the Program to accomplish their described Program roles.

The requirement and rationale for and the anticipated use or integration of Government resources, including but not limited to all equipment, facilities, information, etc., are fully described including dates when such Government Furnished Property (GFP), GFE, GFC, GFI or other similar Government-provided resources shall be required.

The Offeror's RDMP is complete, addressing the types of data to be collected or produced, describing how each type of data will be preserved and shared, including plans to provide public access to peer reviewed publications and the underlying Research Data, or provides justifiable rationale for not making this data available.

5.A.1.c. Contribution and Relevance to the IARPA Mission and Program Goal

The proposed solution meets the letter and intent of the stated program goals and all elements within the proposal exhibit a comprehensive understanding of the problem. The Offeror clearly addresses how the proposed effort shall meet and progressively demonstrate the Program goals. The Offeror describes how the proposed solution contributes to IARPA's mission to invest in high-risk/high-payoff research that can provide the U.S. with an overwhelming intelligence advantage.

The Offeror's proposed IP and data rights are consistent with the Government's need to be able to effectively manage the program and evaluate the technical output and deliverables, communicate program information across Government organizations and support transition to and further use and development of the program results by IC users and others at a reasonable cost that is acceptable to the Government. The proposed approach to IP rights is in the Government's best interest.

5.A.1.d Relevant Experience and Expertise

The Offeror's capabilities, related experience, facilities, techniques, or unique combination of these, which are integral factors for achieving the proposal's objectives, shall be evaluated, as well as qualifications, capabilities, and experience of all Key Personnel and significant contributors critical in achieving the program objectives.

5.A.1.e Resource Realism

The proposed resources demonstrate a clear understanding of the program, a perception of the risks and the Offeror's ability to organize and perform the work. The labor hours and mix are consistent with the technical approach and are realistic for the work proposed. Material, equipment, software, data collection and management, and travel, especially foreign travel, are well justified, reasonable, and required for successful execution of the proposed work.

5.A.2. Funding Availability Factor

5.A.2.a. Budget Constraints

The Government will seek to maximize the likelihood of meeting program objectives within program budget constraints. This may involve awarding one or more contracts. **Note:** If the Offeror has submitted the proposal to other federal, state, or local agencies or other parties that may fund the proposed effort, it may impact the Government's decision to fund the effort.

5.A.2.b. Program Balance

The Government will consider IARPA's overall mission and program objectives, which may include but are not limited to the following: broadening the variety of technical approaches to enhance program outcomes, transitioning the technology to Government partners, developing capabilities aligned with the priorities of the IC and national security.

5.B. Method of Evaluation and Selection Process

The Government will conduct an impartial, equitable, comprehensive proposal reviews and selects the source (or sources) whose offer meets the Government's technical, policy and programmatic goals. For evaluation purposes, a proposal is the document described in Section 4 of the BAA. Other supporting or background materials submitted with the proposal shall not be considered.

The contract award process for this BAA has two steps. The first step is selection for negotiations and is made based on review of the technical and funding availability factors (See BAA Section 5.A.). The second step is negotiation and contract award. Contract award is contingent on Contracting Officer determination of a fair and reasonable cost/price and agreement on terms and conditions.

Selection for negotiation, will be conducted through a peer or scientific review process led by the PM. This process entails establishing a Scientific Review Panel (SRP) made up of qualified Government personnel who will review and assess each proposal's strengths, weaknesses, and risks against the technical evaluation criteria. If necessary, non-Government technical experts with specialized expertise may advise Government panel members and the PM. However, only Government personnel will make selection determinations under this BAA.

Proposals will be reviewed individually and will not be reviewed against each other as they are not submitted in accordance with a common SOW. When SRP reviews are complete, the PM will prepare a recommendation to the IARPA Scientific Review Official (SRO) identifying proposals as selectable, selectable with modification, or not selectable based on consideration of all stated factors (technical and funding availability factors). The SRO will make the final decision as to selectability for negotiations. At this point, Offerors will be notified in writing as to whether they have been determined selectable, selectable with modification, or not selectable.

5.C. Negotiation and Contract Award

After selection and before award, the Government will contact Offerors whose proposals were selected or selected with modifications to engage in negotiations. At that time, the Government will also request a full cost proposal, as described in BAA Section 4.B.2. The Government will review the cost proposal using the proposal analysis techniques described in FAR 15.404-1, as appropriate, to determine a fair and reasonable cost. The Government's evaluation will include review of proposed anticipated costs/prices of the Proposer and those of associate, participating organizations, to ensure the Offeror has fully analyzed the budget requirements, provided sufficient supporting information, has adequate systems for managing the contract (accounting, purchasing), and that data is traceable and reconcilable. The Government will also determine

whether the prospective contractor meets the responsibility standards of FAR Section 9.104. Additional information and supporting data may be requested.

If proposed costs submitted are substantially different than the estimates provided in the technical proposal, then a contract may not be awarded.

Procurement contracts, as determined by the contracting officer, shall be awarded to those Offerors whose proposals are deemed most advantageous to the Government, all stated evaluation factors considered, and pending the successful conclusion of negotiations.

5.D. Proposal Retention

Proposals shall not be returned upon completion of the source selection process. The original of each proposal received shall be retained by the Government and all other non-required copies shall be destroyed. A certification of destruction may be requested, provided that the formal request is sent to the Government via e-mail to dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov within 5 days after notification of proposal results.

6. AWARD ADMINISTRATION INFORMATION

6.A. Award

6.A.1. Communications and Award Notices

All questions or discussions regarding this solicitation must be directed to the Contracting Officer. All communication throughout this process must be handled formally and through the proper channels, which means all parties must ensure a Government Contract Specialist or Contracting Officer is present and/or engaged during any and all communication exchanges. Any informal communications or outside communication will delay and may also jeopardize a potential award.

As soon as practicable after the evaluation of a proposal is complete, the Offeror will be notified that: (1) its proposal has been selected for negotiations, or (2) its proposal has not been selected for negotiations.

6.A.2. Types of Awards

Procurement contracts will be made under this announcement. There are no limits on award amounts.

6.A.3. Offer Preparation Reimbursement

The Government provides no funding for direct reimbursement of proposal development costs.

6.A.4. Obligating of the Government

Prospective Offerors are advised that only Contracting Officers are legally authorized to commit the Government. Only Contracting Officers may obligate the Government to an agreement involving the expenditure of Government funds. Any resultant procurement contract award would include all clauses required by the FAR and appropriate supplements.

6.A.5. Security Guidance

Security classification guidance via a DD Form 254, "DoD Contract Security Classification Specification," will not be provided at this time since the Government is soliciting ideas only. After reviewing the incoming proposals, if a determination is made that the award instrument may result in access to classified information, then a DD Form 254 will be issued and attached as part of the award. Depending on the work to be performed, the Offeror may require a SECRET facility clearance and safeguarding capability; therefore, personnel identified for assignment to a classified effort must be cleared for access to SECRET information at the time of award. In addition, the Offeror may be required to have, or have access to, a certified and Government-approved facility to support work under this BAA.

6.A.6. Proposal Handling

The Government has contracted for various business and staff support services, some of which require contractors to obtain access to proprietary information submitted by Offerors. Any objection to access must be in writing to the Contracting Officer and shall include a detailed statement of the basis for the objection.

6.A.7. Offer Markings

The government prefers that Offerors not include proprietary data in the Technical Proposals and associated attachments. However, if an Offeror deems it necessary to include proprietary information, then proprietary data should have the cover page and each page containing proprietary data clearly marked as containing proprietary data. If only portions of the page contain proprietary information, then those specific portions should be clearly marked. It is the Proposer's responsibility to clearly define to the Government what is considered proprietary data. No proposals containing classified information should be submitted under this announcement.

6.A.8. Small Business Innovation Research (SBIR)

Offerors may propose perform work that is a continuation of a previously awarded SBIR research project. However, Offerors shall not receive duplicative funding (i.e., no SBIR awardee may be paid twice to perform the same task).

6.B. Other Administrative Information

6.B.1. Export Control

Offerors are warned that compliance with International Traffic in Arms Regulations (ITAR) may be required and will be included in all procurement contracts. The ITAR, issued by the Dept. of

State, controls the export of defense-related articles and services, including technical data, ensuring compliance with the Arms Export Control Act (22 U.S.C. 2751 et seq.) If a Proposer has questions regarding how to comply with the ITAR, they are directed to look at DFARS 252.225-7048€.

Offerors are also warned that compliance with the Export Administration Regulations (EAR) may be required and will be included in all procurement contracts. The EAR, issued by the Dept. of Commerce, controls the export of dual-use times, (items that have both commercial and military or proliferation applications) and purely commercial items. These items include commodities, software, and technology. Refer to the Commerce Control List, which is part of the EAR, to identify items subject to EAR, at http://www.gpoaccess.gov/cfr/index.html and http://www.access.gpo.gov/bis/ear/ear_data.html.

The following clause, DFARS 252.225-7048 – Export-Controlled Items, will be included in awards as deemed appropriate:

(e) Definition. "Export-controlled items," as used in this clause, means items subject to the Export Administration Regulations (EAR) (15 CFR Parts 730-774) or the International Traffic in Arms Regulations (ITAR) (22 CFR Parts 120-130). The term includes:

(1) "Defense items," defined in the Arms Export Control Act, 22 U.S.C. 2778(j)(4)(A), as defense articles, defense services, and related technical data, and further defined in the ITAR, 22 CFR Part 120.
(2) "Items," defined in the EAR as "commodities", "software", and "technology," terms that are also defined in the EAR, 15 CFR 772.1.

(b) The Contractor shall comply with all applicable laws and regulations regarding export-controlled items, including, but not limited to, the requirement for contractors to register with the Department of State in accordance with the ITAR. The Contractor shall consult with the Department of State regarding any questions relating to compliance with the ITAR and shall consult with the Department of Commerce regarding any questions relating to compliance with the EAR.

€ The Contractor's responsibility to comply with all applicable laws and regulations regarding export-controlled items exists independent of, and is not established or limited by, the information provided by this clause.

(d) Nothing in the terms of this contract adds, changes, supersedes, or waives any of the requirements of applicable Federal laws, Executive orders, and regulations, including but not limited to—
(1) The Export Administration Act of 1979, as amended (50 U.S.C. App. 2401, et seq.);
(2) The Arms Export Control Act (22 U.S.C. 2751, et seq.);
(3) The International Emergency Economic Powers Act (50 U.S.C. 1701, et seq.);
(4) The Export Administration Regulations (15 CFR Parts 730-774);
(5) The International Traffic in Arms Regulations (22 CFR Parts 120-130); and
(6) Executive Order 13222, as extended.

€ The Contractor shall include the substance of this clause, including this paragraph €, in all subcontracts.

6.B.2. Public Release

It is the policy of the Department of Defense that the publication of products of fundamental research will remain unrestricted to the maximum extent possible. Research to be performed as a result of this BAA may be Fundamental. The Government does not anticipate applying publication restrictions of any kind, but reserves the right to require prior review before publication in appropriate or required circumstances.

Offerors should note that pre-publication approval of certain information may be required if it is determined that its release may result in the disclosure of sensitive intelligence information.

A courtesy soft copy of any work submitted for publication shall be provided to the IARPA PM and the Contracting Officer Representative (COR) a minimum of 5 business days prior to release in any forum.

6.B.3. Electronic Systems

6.B.3.a. System for Award Management (SAM)

In accordance with FAR 52.204-7 and DFARS 252.204-7004, an Offeror must be actively registered in the System for Award Management. Selected Offerors not already registered in SAM will be required to register prior to any award under this BAA. FAR 52.204-7 System for Award Management and FAR 52.204-13 System for Award Management Maintenance are incorporated into this BAA, and FAR 52.204-13 will be incorporated in all awards. Information on SAM registration is available at https://www.sam.gov/portal/public/SAM/

6.B.3.b. Representations and Certifications

In accordance with FAR 4.1201, prospective Proposers shall complete electronic annual representations and certifications at https://www.sam.gov/portal/public/SAM/

6.B.3.c. Invoicing, Receipt, Acceptance, and Property Transfer (iRAPT) (formerly Wide Area Work Flow (WAWF))

Unless using another approved electronic invoicing system, Performers will be required to submit invoices for payment directly via the Internet/WAWF at https://wawf.eb.mil. Registration to iRAPT/WAWF will be required prior to any award under this BAA.

6.B.4. Certificate of Current Cost and Pricing Data

Upon completion of negotiations and agreement on contract cost, a Certificate of Current Cost or Pricing Data may be required in accordance with FAR 15.406-2. In addition, any Offeror who is required to submit and certify cost or pricing data shall certify on behalf of subcontractors.

Additional Contractual Requirements

If an Offeror and the Government accepts an Offeror's proposal to use government resources in performance of an award (e.g., GFP, GFI, GFE, GFC etc.), the resultant award will include additional contractual requirements. The specific requirements will be determined for the individual award.

6.B.5. Use of Arms, Ammunition and Explosives

Safety

The Offeror is required to be in compliance with DoD manual 4145.26-M, DoD Contractor's Safety Manual for Ammunition and Explosives if ammunitions and/or explosives are to be utilized under the proposed research effort. (See DFARS 223.370-5 and DFARS 252.223-7002)

If ammunitions and/or explosives (A&E) are to be utilized under the proposed research effort, the Government requires a preaward safety survey in accordance with DFARS PGI 223.370-4(C)(iv) entitled Preaward survey. The Offeror is solely responsible for contacting the cognizant Defense Contract Management Agency (DCMA) office and obtaining a required preaward safety survey before proposal submission. The Offeror should include required preaward safety surveys with proposal submissions.

If the Offeror proposes that the Government provide Government-furnished A&E containing any nitrocellulose-based propellants and/or nitrate ester-based materials (such as nitroglycerin) or other similar A&E with a tendency to become chemically unstable over time, then NMCARS 5252.223-9000 will also apply to a resulting contract award. (See NMCARS 5223.370-5)

Security

If arms, ammunition, or explosives (AA&E) are to be utilized under the proposed research effort, the Government requires a preaward security survey. The Offeror is solely responsible for contacting the cognizant DCMA office and obtaining a required preaward security survey before proposal submission. The Offeror should include a required preaward security survey with proposal submission. (See DoD manual 5100.76-M, Physical Security of Sensitive Conventional Arms, Ammunition and Explosives, paragraph C1.3.1.4)

If AA&E are to be utilized under the proposed research effort, the Government may require the Contractor to have perimeter fencing around the place of performance in accordance with DoD 5100.76-M, Appendix 2.

If AA&E are to be utilized under the proposed research effort, the Offeror is required to provide a written copy of the Offeror's AA&E accountability procedures in accordance with DoD 5100.76-M. If the Offeror is required to provide written AA&E accountability procedures, the Offeror should provide the respective procedures with its proposal submission. See DoD 5100.76-M Appendix 2.12.

6.B.6. Employment Eligibility Verification (E-verify)

As per FAR 22.1802, recipients of FAR-based procurement contracts must enroll as Federal Contractors in E-verify and use E-verify to verify employment eligibility of all employees assigned to the award. All resultant contracts from this solicitation will include FAR 52.222-54, "Employment Eligibility Verification."

6.B.7. Reporting

Fiscal and management responsibility are important to the Program. Although the number and types of reports shall be specified in the award document, all Offerors shall, at a minimum, provide the CO, COTR and PM with monthly technical reports and monthly financial reports. The reports shall be prepared and submitted in accordance with the procedures contained in the award document and mutually agreed upon before award. Technical reports shall describe technical highlights and accomplishments, priorities and plans, issues and concerns, evaluation results, and future plans. Financial reports shall present an on-going financial profile of the project, including total project funding, funds invoiced, funds received, funds expended during the preceding month, and planned expenditures over the remaining period. Additional reports and briefing material may also be required, as appropriate, to document progress in accomplishing program metrics.

The Offeror shall prepare and provide a research report of their work by month 18 for Phase 1, by month 12 for Phase 2, and month 12 for Phase 3. The reports shall be delivered to the CO, COTR and the PM. The reports shall include:

- Problem definition
- Findings and approach
- System design
- Possible generalization(s)
- Information on performance limitations and potential mitigation
- Anticipated path ahead
- Lessons learned (technical and programmatic)
- Final identification of all commercial, third-party, or proprietary hardware, software, or technical data integrated into any deliverable and all applicable use restrictions.
- Any research products, including publications, data, and software, resulting from the project during the reporting period. The final report shall list in-progress scientific manuscripts and other research products.

6.B.8. Human Use

All research involving human subjects, to include use of human biological specimens and human data, selected for funding must comply with the federal regulations (45 CFR 46) for human subject protection. Further, research involving human subjects that is conducted or supported by the DoD must comply with 32 CFR 219, Protection of Human Subjects (http://www.ecfr.gov/cgi-bin/text-idx?tpl=/ecfrbrowse/Title32/32cfr219_main_02.tpl), DoD Directive 3216.02, Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research

(http://www.dtic.mil/whs/directives/corres/pdf/321602p.pdf) and Department of Navy (DoN) Instruction SECNAVINST 3900.39E CH-1.

Proposers should also be aware that selected performer contracts will be awarded from NIWC Pacific (A DoD command), and as such the awarded contracts will be considered DOD supported research. Any DOD supported contracts that include human subject research are subject to oversight by a Government appointed Human Research Protection Official (HRPO). Prior to any work performed with humans as test subjects, the Performer will be required to obtain not only their Institutional Review Board (IRB) approvals, but also NIWC Pacific HRPO approval.

Institutions receiving funded awards that include research involving human subjects must provide documentation of a current institutional Assurance of Compliance with Federal regulations for human subject protection. A Federal Wide Assurance (FWA) example can be found at Department of Health and Human Services, Office of Human Research Protection (http://www.hhs.gov/ohrp). All institutions engaged in human subject research, to include subcontractors, must also have a valid Assurance. In addition, personnel involved in human subject research must provide documentation of completing appropriate training for the protection of human subjects.

For all proposed research that will involve human subjects in the first year or phase of the project, the Proposer must provide evidence of, or a plan for, review by an Institutional Review Board (IRB) upon final proposal submission to NIWC Pacific. The IRB conducting the review must be the IRB identified on the institution's Assurance. The protocol, separate from the proposal, must include a detailed description of the research plan, study population, risks and benefits of study participation, recruitment and consent process, data collection, and data analysis. See Appendix A.7 for a template of the IRB information that should be included in proposals with experimental protocol submissions, as well as standard language for use in IRB submissions. The informed consent document must comply with both federal (45 CFR 46.117) and DoD regulations (32 CFR 219.116). A valid Assurance along with evidence of appropriate training of all investigators should accompany the protocol for review by the IRB.

Special DoD Considerations

For DoD-supported research in which the proposer believes it is exempt, or does not constitute human subject research, they will be required to submit institutional documentation of this determination to NIWC Pacific HRPO for concurrence. A determination of non-HSR or exempt-HSR must be made by the Proposer's IRB. All protocol documentation, including final IRB determination letter, will be required for submission to obtain HRPO concurrence.

For all non-exempt human subject research, the selected Performer will be required to provide documentation of a scientific review in the initial IRB package submitted for HRPO review. The SECNAVINST 3900.39E CH-1 defines a scientific review as an independent review of the IRB protocol conducted prior to IRB review (i.e., independent of the IRB review process). It can be conducted in a variety of ways appropriate to the research and institution (e.g., by committee, board, or single knowledgeable individual). However, the Government's selection of proposal for negotiation does not merit a scientific review. At a minimum, scientific review must meet applicable conflict of interest rules and regulations, and should consider: human research

significance, adequacy of research approach; and competency of the investigator performing the research. In addition, written Command approval is required for all research intending to use military and/or DoD civilian subjects as part of their study. Documentation of this Command approval should be included in the IRB protocol package prior to a Performer's IRB approval. The Performer should consult points of content from individual Army, Navy, or Air Force Commands that are intended to be associated with subject recruitment for obtaining recruitment approval guidance specific to that Command, if applicable.

The amount of time required to complete the IRB review/approval process may vary depending on the complexity of the research and/or the level of risk to study participants. Ample time should be allotted to complete the approval process. The initial Performer IRB approval process can last between one to three months, followed by a DoD review that could last between one to two months for initial review, and up to 30 days for review of each IRB amendment approval. No DoD funding can be placed on a contract toward human subject tasking until ALL approvals are granted and documentation has been provided to NIWC Pacific for compliance verification and approval. Proposals must separate out tasking and cost associated with human subject research to clearly delineate which tasks and costs are associated with HSR.

6.B.9. Animal Use

No research proposals involving animal subjects shall be accepted under this BAA. Use of non-human primates is not permitted under this BAA.

6.B.10. Recombinant DNA

Proposals which call for experiments using recombinant DNA must include documentation of compliance with Department of Health and Human Services (DHHS) recombinant DNA regulations, approval of the Institutional Biosafety Committee (IBC), and copies of the DHHS Approval of the IBC letter.

6.B.11. Institutional Dual Use Research of Concern

As of September 24, 2015, all institutions and USG funding agencies subject to the United States Government Policy for Institutional Oversight of Life Sciences Dual Use Research of Concern must comply with all the requirements listed therein. If your research proposal directly involves certain biological agents or toxins, contact the cognizant Technical Point of Contact. U.S. Government Science, Safety, Security (S3) guidance may be found at http://www.phe.gov/s3/dualuse.

6.B.12. Electronic and Information Technology

All electronic and information technology acquired through the BAA must satisfy the accessibility requirements of Section 508 of the Rehabilitation Act (29 U.S.C. § 794d) and FAR Subpart 39.2. Each Proposer who submits a proposal involving the creation or inclusion of electronic and information technology must ensure that Federal employees with disabilities will have access to

and use of information that is comparable to the access and use by Federal employees who are not individuals with disabilities. Additionally, each Proposer must ensure that members of the public with disabilities seeking information or services from NIWC Pacific will have access to and use of information and data that is comparable to the access and use of information and data by members of the public who are not individuals with disabilities.

6.C. FAR / DFARS Provisions & Clauses

6.C.1. Provisions

For purposes of illustration and not limitation, the following provisions/clauses may be applicable to NIWC Pacific contracts resulting from this BAA:

FAR Clause No.	Title
52.204-8	Annual Representations and Certifications
52.204-16	Commercial and Government Entity Code Reporting
52.204-22	Alternative Line Item Proposal
52.204-24	Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment
52.209-7	Information Regarding Responsibility Matters
52.209-13	Violation of Arms Control Treaties or Agreements—Certification
52.215-16	Facilities Capital Cost of Money
52.215-22	Limitations on Pass-Through Charges—Identification of Subcontract Effort
52.216-1	Type of Contract
52.216-27	Single or Multiple Awards
52.217-4	Evaluation of Options Exercised at Time of Contract Award
52.217-5	Evaluation of Options
52.229-11	Tax on Certain Foreign Procurements—Notice and Representation.
52.230-1	Cost Accounting Standards Notices and Certification
52.230-7	Proposal Disclosure—Cost Accounting Practice Changes
52.233-2	Service of Protest
52.252-1	Solicitation Provisions Incorporated by Reference
52.252-5	Authorized Deviations in Provisions

DFARS Clause No.	Title
252.203-7005	Representation Relating to Compensation of Former DoD Officials
252.204-7007	Alternate A, Annual Representations and Certifications
252.204-7008	Compliance with Safeguarding Covered Defense Information Controls
252.204-7016	Covered Defense Telecommunications Equipment or Services--Representation
252.204-7017	Prohibition on the Acquisition of Covered Defense Telecommunications Equipment or Services--Representation
252.204-7019	Notice of NIST SP 800-171 DoD Assessment Requirements.

252.215-7003	Requirement for Submission of Data Other Than Certified Cost or Pricing Data—Canadian Commercial Corporation
252.215-7007	Notice of Intent to Resolicit
252.215-7009	Proposal Adequacy Checklist
252.215-7010	Requirements for Certified Cost or Pricing Data and Data Other Than Certified Cost or Pricing Data--Basic
252.215-7011	Requirements for Submission of Proposals to the Administrative Contracting Officer and Contract Auditor
252.215-7012	Requirements for Submission of Proposals via Electronic Media
252.215-7013	Supplies and Services Provided by Nontraditional Defense Contractors
252.225-7003	Report of Intended Performance Outside the United States and Canada—Submission with Offer
252.225-7032	Waiver of United Kingdom Levies—Evaluation of Offers
252.225-7973	Prohibition on the Procurement of Foreign-Made Unmanned Aircraft Systems—Representation. (DEVIATION 2020-O0015)
252.225-7974	Representation Regarding Persons that have Business Operations with the Maduro Regime (DEVIATION 2020-O0005)
252.227-7013	Rights in Technical Data—Other Than Commercial Products and Commercial Services
252.227-7014	Rights in Other Than Commercial Computer Software and Other Than Commercial Computer Software Documentation
252.227-7016	Rights in Bid or Proposal Information
252.227-7017	Identification and Assertion of Use, Release, or Disclosure Restrictions
252.227-7020	Rights in Special Works
252.227-7028	Technical Data or Computer Software Previously Delivered to the Government
252.227-7030	Technical Data—Withholding of Payment
252.235-7004	Protection of Human Subjects
252.235-7010	Acknowledgment of Support and Disclaimer
252.239-7098	Prohibition on Contracting to Maintain or Establish a Computer Network Unless Such Network is Designed to Block Access to Certain Websites--Prepresention
252.247-7022	Representation of Extent of Transportation by Sea

6.C.2. Clauses

FAR and DFARS clauses apply to any contract awarded under this BAA. Specific clauses depend on a variety of factors (e.g., contract type, contract value, business size, etc.) and will be negotiated at award.

6.C.2.a. Combating Trafficking in Persons

Appropriate language from FAR Clause 52.222-50 will be incorporated in all awards.

6.C.2.b. Ensuring Adequate COVID-19 Safety Protocols for Federal Contractors

DFARS Clause 252.223-7999 Ensuring Adequate COVID-19 Safety Protocols for Federal Contractors (DEVIATION 2021-O0009) will be incorporated in all awards.

6.C.2.c. Certification Regarding Trafficking in Persons Compliance Plan

Prior to award of a contract, for the portion of the contract that is for supplies, other than commercially available off-the-shelf items, to be acquired outside the United States, or services to be performed outside the United States, and which has an estimated value that exceeds $500,000, the contractor shall submit the certificate as specified in paragraph (c) of 52.222-56, Certification Regarding Trafficking in Persons Compliance Plan.

6.C.2.d. Updates of Information regarding Responsibility Matters

FAR clause 52.209-9, "Updates of Publicly Available Information Regarding Responsibility Matters", will be included in all contracts valued at $500,000 where the contractor has current active Federal contracts and grants with total value greater than $10,000,000.

VII. AGENCY CONTACTS:

Questions of a technical and/or business nature shall be submitted to the Contracting Officer via email to dni-iarpa-rescind-BAAsubmission-2023@iarpa.gov.

Questions must reference the title and number of the BAA.

This notice constitutes a BAA as contemplated in FAR 35.016. No additional written information is available, nor will a formal request for proposal (RFP) or other solicitation regarding this announcement be issued. Interested parties are invited to respond to this announcement. All responsible parties' responses will be considered.

Appendix A: Templates for Volume 1: Technical Proposal

A.1 Cover Sheet for Volume 1: Technical Proposal

(1) BAA Number	**N66001-23-S-4510**
(2) Technical Challenge(s) – (TC)(s), if applicable	
(3) Lead Organization Submitting Proposal	
(4) Type of Business, Selected Among the Following Categories: "Large Business", "Small Disadvantaged Business", "Other Small Business", "HBCU", "MI", "Other Educational", or "Other Nonprofit"	
(5) Contractor's Reference Number (if any)	
(6) Other Team Members (if applicable) and Type of Business for Each	
(7) Proposal Title	
(8) Technical Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(9) Administrative Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(10) Volume 1 no more than the specified page limit	Yes/No
(11) Restrictions on Intellectual property rights details provided in Appendix A format?	Yes/No
(12) Research Data Management Plan included?	Yes/No
(13) OCI Waiver Determination, Notification or Certification [see Section 3 of the BAA] Included?	Yes/No
(13a) If No, is written certification included (Appendix A)?	Yes/No
(14) Are one or more U.S. Academic Institutions part of your team?	Yes/No
(14a) If Yes, are you including an Academic Institution Acknowledgment Statement with your proposal for each U.S. Academic Institution that is part of your team (Appendix A)?	Yes/No
(15) Total Funds Requested from IARPA and the Amount of Cost Share (if any)	$
(16) Date of Proposal Submission	

Appendix A.2 Academic Institution Acknowledgment Letter

-- Please Place on Official Letterhead --

<Insert date>

To: Contracting Officer
NIWC Pacific

Office of the Director of National Intelligence
Washington, D.C. 20511

Subject: Academic Institution Acknowledgment Letter Reference: Executive Order 12333, As Amended, Para 2.7

This letter is to acknowledge that the undersigned is the responsible official of <insert name of the academic institution>, authorized to approve the contractual relationship in support of the Office of the Director of National Intelligence's Intelligence Advanced Research Projects Activity and this academic institution.

The undersigned further acknowledges that he/she is aware of the Intelligence Advanced Research Projects Activity's proposed contractual relationship with <insert name of institution> through N66001-23-S-4510 and is hereby approved by the undersigned official, serving as the president, vice-president, chancellor, vice-chancellor, or provost of the institution.

<Name> Date

<Position>

Appendix A.3 Intellectual Property Rights

[Please provide here your good faith representation of ownership or possession of appropriate licensing rights to all IP that shall be utilized under the Program.]

Patents

PATENTS				
Patent number (or application number)	Patent name	Inventor name(s)	Patent owner(s) or assignee	Incorporation into deliverable
(LIST)	(LIST)	(LIST)	(LIST)	(Yes/No; applicable deliverable)

(1) Intended use of the patented invention(s) listed above in the conduct of the proposed research:
(2) Description of license rights to make, use, offer to sell, or sell, if applicable, that are being offered to the Government in patented inventions listed above:
(3) How the offered rights will permit the Government to reach its program goals (including transition) with the rights offered:
(4) Cost to the Government to acquire additional or alternative rights, if applicable:
(5) Alternatives, if any, that would permit IARPA to achieve program goals:

Data (Including Technical Data and Computer Software)

NONCOMMERCIAL ITEMS			
Technical Data, Computer Software To be Furnished With Restrictions	**Basis for Assertion**	**Asserted Rights Category**	**Name of Person Asserting Restrictions**
(LIST)	(LIST)	(LIST)	(LIST)

COMMERCIAL ITEMS			
Technical Data, Computer Software To be Furnished With Restrictions	**Basis for Assertion**	**Asserted Rights Category**	**Name of Person Asserting Restrictions**
(LIST)	(LIST)	(LIST)	(LIST)

(1) Intended use of the data, including, technical data and computer software, listed above in the conduct of the proposed research:
(2) Description of Asserted Rights Categories, specifying restrictions on Government's ability to use, modify, reproduce, release, perform, display, or disclose technical data, computer software, and deliverables incorporating technical data and computer software listed above:
(3) How the offered rights will permit the Government to reach its program goals (including transition) with the rights offered:
(4) Cost to the Government to acquire additional or alternative rights, if applicable:
(5) Alternatives, if any, that would permit IARPA to achieve program goals:

Appendix A.4 Organizational Conflicts of Interest Certification Letter

(Month DD, YYYY)

Office of the Director of National Intelligence

Intelligence Advanced Research Projects Activity (IARPA) ReSCIND Program

ATTN: Eric Pomroy, NIWC Pacific, Contracting Officer

Subject: OCI Certification

Reference: <Insert Program Name>, N66001-23-S-4510, (Insert assigned proposal ID#, if received)

Dear_____,

In accordance with Broad Agency Announcement N66001-23-S-4510, Organizational Conflicts of Interest (OCI), and on behalf of (Offeror name) I certify that neither (Offeror name) nor any of our subcontractor teammates has as a potential conflict of interest, real or perceived, as it pertains to the ReSCIND program. Please note the following subcontractors and their proposed roles:

[Please list all proposed contractors by name with a brief description of their proposed involvement.]

If you have any questions, or need any additional information, please contact (Insert name of contact) at (Insert phone number) or (Insert e-mail address).

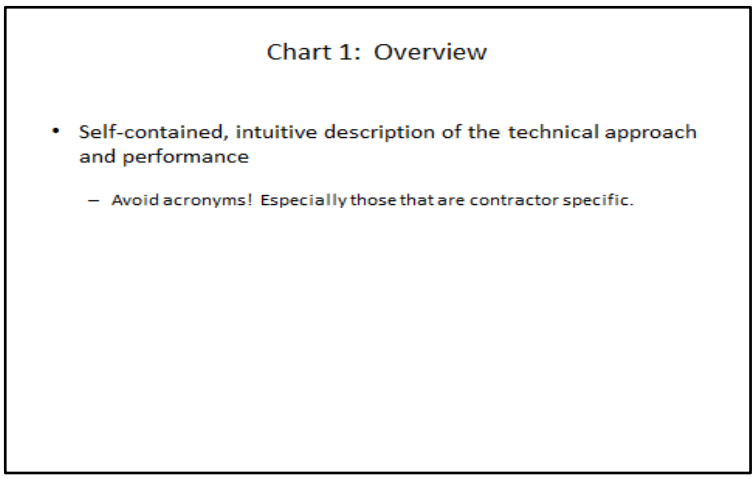
Sincerely,

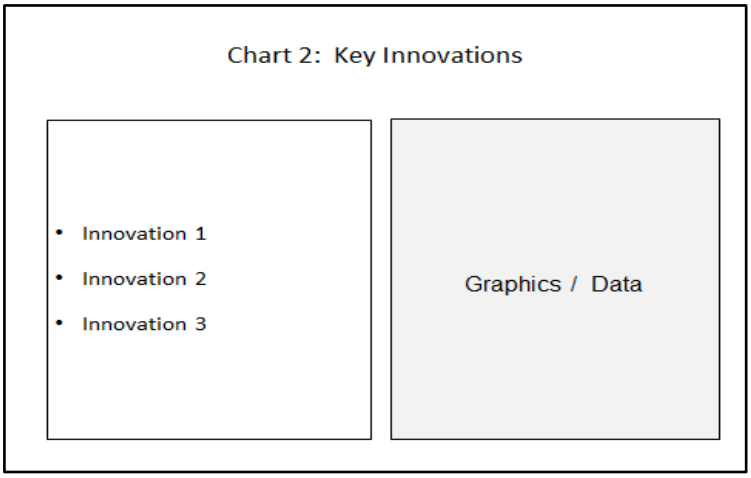
(Insert organization name) (Shall be signed by an official that has the authority to bind the organization)

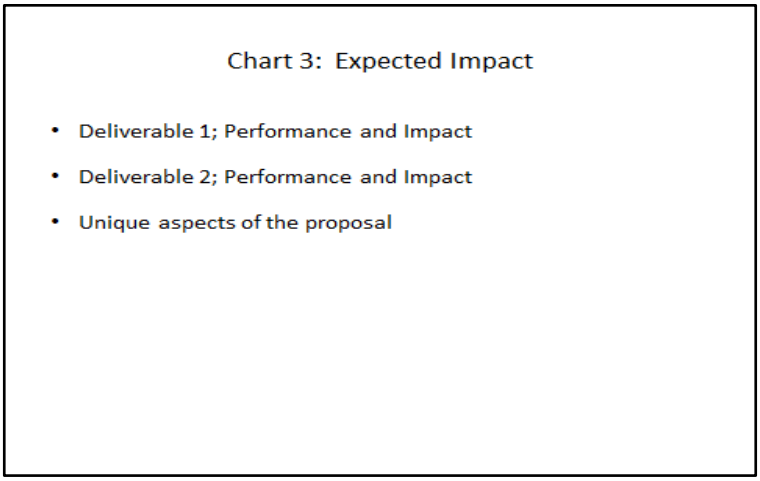
(Insert signature)

(Insert name of signatory)
(Insert title of signatory)

Appendix A.5 Three Chart Summary of the Proposal







Appendix A.6 Research Data Management Plan (RDMP) N66001-23-S-4510

The Offeror must address each of the elements noted below.

The RDMP shall comply with the requirements stated in Section 4 of the BAA. In doing so, it will support the objectives of the ODNI Public Access Plan at https://www.iarpa.gov/index.php/working-with-iarpa/public-access-to-iarpa-research

1. **Sponsoring IARPA Program** (required):
2. **Offeror** (i.e., lead organization responding to BAA) (required):
3. **Offeror point of contact** (required):

The point of contact is the proposed principal investigator (PI) or his/her Designee.

   a. **Name** and **Position**:
   b. **Organization**:
   c. **Email**:
   d. **Phone**:

4. **Research data types** (required):

Provide a brief, high-level description of the types of data to be collected or produced during the project.

5. **Standards for research data and metadata content and format** (required):

Use standards reflecting the best practices of the relevant scientific discipline and research community whenever possible.

6. **Plans for making the research data that underlie the results in peer-reviewed journal articles and conference papers digitally accessible to the public** at the time of publication/conference or within a reasonable time thereafter (required):

The requirement could be met by including the data as supplementary information to a peer reviewed journal article or conference paper or by depositing the data in suitable repositories available to the public.

   a. **Anticipated method(s) of making research data publicly accessible**:
   ___ Provide dataset(s) to publisher as supplementary information (if publishers allow public access)
   ___ Deposit dataset(s) in Data Repository
   ___ Other (specify)_____

   b. **Proposed research data repository or repositories** (for dataset(s) not provided as supplementary information):

   Suitable repositories could be discipline-specific repositories, general purpose research data repositories, or institutional repositories, as long as they are publicly accessible.

   c. **Retention period, at least three years after publication of associated research results**:

   State the minimum length of time the data will remain publicly accessible.

   d. **Submittal of metadata to IARPA**:

   Offerors are required to make datasets underlying the results published in peer-reviewed journal or conferences digitally accessible to the public to the extent feasible. Here, the Proposer should state a commitment to submit metadata on such

datasets to IARPA in a timely manner. Note: This does not supersede any requirements for deliverable data, as the award document may include metadata as a deliverable item.

7. **Policies and provisions for sharing and preservation** (as applicable):

a. Policies and provisions for appropriate protection of privacy, confidentiality, security, and intellectual property:

b. Descriptions of tools, including software, which may be needed to access and interpret the data:

c. Policies and provisions for re-use, re-distribution, and production of derivative works:

8. **Justification for not sharing and/or preserving data underlying the results of peer-reviewed publications** (as applicable):

If, for legitimate reasons, the data cannot be shared and preserved, the plan must include a justification detailing such reasons. Potential reasons may include privacy, confidentiality, security, IP rights considerations; size of data sets; cost of sharing and preservation; time required to prepare the dataset(s) for sharing and preservation.

Appendix A.7 Experimental Plan, Data Sharing Plan, & IRB Recommended Guidelines and Topics

Information required below should be submitted as a separate attachment from the rest of the technical proposal.

If a Proposer will conduct human subjects research as part of the execution of their technical approach, then the proposal submission must include plans for obtaining Institutional Review Board (IRB) approval. IRB approval documents must be provided to the Government, and receive written concurrence and approval from the Government before commencing any human subject research.

Proposals shall include complete outlines and procedures that will be taken during the experiment(s), including Institutional Review Board (IRB) submission materials, recruitment plans, consent forms and preliminary experimental materials.

The information included in the Experimental Plan below is standardized IRB language that should be included in all Performer IRB protocols. Additions can be made to these items as necessary.

Additionally, proposals must include an experimental plan containing the items below and outlining the hypothesis, independent and dependent variables and their operational definitions, research approach and methodology, notional listing of inventories, measurements, and questionnaires, and a data analytical plan.

Performers are not responsible for obtaining IRB approval for T&E evaluation events.

<u>Experimental Plan</u>

- Protocol Title:
    - *Impact of Cognition on Cyber Behavior*
- Principal Investigators/Co-Investigators/Student Investigators:
- Institutional Affiliations of all Investigators:
- Background and Objectives/Purpose and Rationale of the Study:
    - *This study will be conducted as part of the Intelligence Advanced Research Projects Activity (IARPA) Reimagining Security with Cyberpsychology-Informed Network Defenses (ReSCIND) Program. The IARPA ReSCIND program aims to improve cybersecurity by understanding how human cognition impacts cyber behavior and could affect cyber actors' success in network attack activities. Specifically, well-established cognitive patterns, such as loss aversion and the representativeness bias, will be investigated as potentially mitigating factors in the efficacy of cyber attack behavior. This research will contribute to ReSCIND's broader goals of improving cyber defense practices by delaying and thwarting attacks.*
- Related Studies/Prior Relevant Protocol Approvals:

- Specialized Certifications Required for HSR:
- Participant Inclusion/Exclusion Criteria: (add any special populations here)
- Recruitment Criteria/Screening Methods/Population of Interest:
- Recruitment Methods:
- Consent Process/Waivers/ Process to Document Consent in Writing:
- Number of Participants/Sample Size:
- Compensation/Motivation for Participants:
- Potential Risks/Benefits to Participants:
- Study Site/Locations/Setting:
- Technical Description on Experimental Environment/Testbeds/Sensors:
- Description of Variables (Independent/Dependent)/Operational Definitions:
- Study Timelines/Endpoints:
- Detailed Procedures Involved:
- Preliminary Measures/Inventories/Materials:
- Preliminary Experimental Plan:
- Data Collection Details:
- Data Anonymization Plan:
- Risk(s) of delay in IRB approval and mitigation plan:
- Data Collection/Storage/Management/Insurance of Participant Safety:
- Data access, control, dissemination, and usage:

Appendix A.8 Statement of Work (SOW) Template

STATEMENT OF WORK

PROJECT TITLE: *[Insert short title of procurement requirement]*
DATE*: Insert the date of the SOW*

1.0 SCOPE

The 'Scope' section should emphasize the most important/overarching aspects of the requirements rather than minor details. It should identify the objective or purpose of the requirement and it should help the reader understand the magnitude of the effort to be performed. It should also define limitations/boundaries of the contractor's performance responsibilities. The 'scope' section should be consistent with the requirements specified under the 'performance requirements' section (2.0). *Remove this language after completing this section.*

2.0 TECHNICAL REQUIREMENTS

The *'Performance Requirements'* section will detail the technical performance requirements in clear, concise terms. Performance requirements are generally identified as major tasks and subtasks. The below is a sample format that must be catered to the tasking proposed. The inclusion of Options (Phases) must be clearly delineated.

2.1 (Phase A) Task 1- Task Name
- 2.1.1 Sub Task
- 2.1.2 Sub Task
  - 2.1.2.1 Specific Task

2.2 (Phase A) Task 2- Task Name
- 2.2.1 Sub Task

2.3 (Option 1 Phase B) Task 1- Task Name
- 2.3.1 Sub Task

2.4 (Option 1 Phase B) Task 2- Task Name
- 2.4.1 Sub Task

And so forth…

3.0 TRAVEL

The *'Travel'* section will identify the estimated travel needed to perform the tasking, including the travel location/destination, number of trips, number of people, and number of days/nights. It is advantageous to include the word "estimated" (or similar) in this section. This will allow for unanticipated changes to travel during task order performance without having to modify the order. If traveling to foreign countries outside of the continental United States (OCONUS) is required, the following language is mandatory: *Remove this language after completing this section*

Sample Language:

Anticipated travel includes XXX. Destinations and number of meetings may change upon request of the IARPA Program Office. Attendance of reviews, workshops, and meetings are subject to approval by the IARPA Program Manager or as outlined in the BAA.

4.0 PROPERTY REQUIREMENTS

- Identify Property Types Separately: Clearly address GFP items, other GP (Non-GFP) and GFI separately in order to avoid confusion in the SOW and ensure proper Classifications as each classification/type of property is handled differently. Address and explicitly state if none or some of the five (5) property categories are anticipated as follows:
  - Government Furnished Property (GFP). XXX
  - Government Furnished Information (GFI). XXX
  - Government Property (Incidental). XXX
  - Government Furnished Facilities. XXX
  - Contractor Acquired Property (CAP). XXX

Remove any instruction language after completing this section.

5.0 SECURITY

The work performed under this effort is anticipated to be unclassified.

6.0 DELIVERABLES

The *'Deliverables'* provides a summary of deliverables due to the Government. This section may simply make reference to other areas in this SOW and/or a list of the Exhibit A, Contract Data Requirements List (CDRL). This section is encouraged as an overall summary to ensure clarity depending on the complexity of the acquisition/program. This section clearly identifies the tangible products or outcomes that the contractor is required to produce.

- A CDRL listing identifying the data item deliverables required under this contract and the applicable section of the SOW for which they are required will be referenced here and Section J of the resultant contract will include the DD Form 1423s that itemizes each CDRL required under the contract. The contractor shall establish a practical and cost-effective system for developing and tracking the required CDRLs generated under each task. Sample summary Table: *Remove this language after completing this section*

CDRL * #	Deliverable Title	SOW Ref Para	Frequency	Date Due	Security Classification (up to S/TS or unclassified)
A###		2.#			
A###		2.#			

The government will complete the first column.

7.0 DATA RIGHTS REQUIREMENTS

At a minimum, the Government requires the following rights:

a. The rights to use, modify, reproduce, release, perform, display, or disclose delivered data within the Government, without restrictions, and to disclose the data outside the Government and authorize persons to whom release or disclosure has been made, to use, modify, reproduce, release, perform, display, or disclose that data or software for any United States Government purpose, without the recipient's permission.

b. Note: Anything less than government purpose rights that is identified in negotiation having the potential to impair transition of IARPA developed technology from Phase 1 to Phase 2 should be returned to IARPA for consideration.

c. In accordance with DFARS Clause No. 252.227-7013 Rights in Technical Data—Noncommercial Items., the Contractor asserts for itself, or the persons identified below, that the Government's rights to use, release, or disclose the following technical data should be restricted—

Technical Data to be Furnished with Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****
(LIST)	(LIST)	(LIST)	(LIST)

Remove asterisks and below language once completing the list.

**If the assertion is applicable to items, components, or processes developed at private expense, identify both the data and each such item, component, or process.*

***Generally, the development of an item, component, or process at private expense, either exclusively or partially, is the only basis for asserting restrictions on the Government's rights to use, release, or disclose technical data pertaining to such items, components, or processes. Indicate whether development was exclusively or partially at private expense. If development was not at private expense, enter the specific reason for asserting that the Government's rights should be restricted.*

****Enter asserted rights category (e.g., government purpose license rights from a prior contract, rights in SBIR data generated under another contract, limited or government purpose rights under this or a prior contract, or specifically negotiated licenses).*

*****Corporation, individual, or other person, as appropriate. Include subcontractor assertions as applicable.*

8.0 PLACE AND PERIOD OF PERFORMANCE

Sample Language

The place of performance for the work is XXX.

The period of performance is:
Phase 1: XXX
Phase 2: XXX
Phase 3: XXX

Appendix B: Templates for Volume 2: Cost Proposal

Appendix B.1 Cover Sheet for Volume 2: Cost Proposal

(1) BAA Number	**N66001-23-S-4510**
(2) Technical Challenge(s) (TC)(s)	
(3) Lead organization submitting proposal	
(4) Type of Business, Selected Among the Following Categories: "Large Business", "Small Disadvantaged Business", "Other Small Business", "HBCU", "MI", "Other Educational", or "Other Nonprofit"	
(5) Contractor's Reference Number (if any)	
(6) Other Team Members (if applicable) and Type of Business for Each	
(7) Proposal Title	
(8) Technical Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(9) Administrative Point of Contact to Include: Title, First Name, Last Name, Street Address, City, State, Zip Code, Telephone, Fax (if available), Electronic Mail (if available)	
(10) Contract type/award Instrument Requested: specify	
(11) Place(s) and Period(s) of Performance	
(12) Total Proposed Cost Separated by Basic Award and Option(s) (if any)	
(13) Name, Address, Telephone Number of the Offeror's Defense Contract Management Agency (DCMA) Administration Office or Equivalent Cognizant Contract Administration Entity, if Known	
(14) Name, Address, Telephone Number of the Offeror's Defense Contract Audit Agency (DCAA) Audit Office or Equivalent Cognizant Contract Audit Entity, if Known	
(15) Date Proposal was Prepared	
(16) DUNS Number	
(17) TIN Number	
(18) CAGE Code	
(19) Proposal Validity Period [minimum of 180 days]	
(20) Cost Summaries Provided (Appendix B)	
(21) Size of Business in accordance with NAICS Code 541712	

Appendix B.2 Prime Contractor/Subcontractor Cost Element Sheet for Volume 2: Cost Proposal

Prime Contractor/Subcontractor Cost Element Sheet for Volume 2: Cost Proposal			
Complete a Cost Element Sheet for the Base Period and each Option Period			
COST ELEMENT	BASE	RATE	AMT
DIRECT LABOR (List each labor category separately. Identify all Key	# of Hours	$	$
TOTAL DIRECT LABOR			$
FRINGE BENEFITS	$	%	$
TOTAL LABOR OVERHEAD	$	%	$
SUBCONTRACTORS, IOTS, CONSULTANTS			$
MATERIALS & EQUIPMENT (List each material and equipment item separately.)	Quantity	$ unit price	$
SOFTWARE & IP (List separately. See table below.)	$	$	$
TOTAL MATERIALS & EQUIPMENT			$
MATERIAL OVERHEAD	$	%	$
TRAVEL (List each trip separately.)	# of travelers	$ price per	$
TOTAL TRAVEL			$
OTHER DIRECT COSTS (List each item separately.)	Quantity	$ unit price	$
TOTAL ODCs			$
G&A	$	%	$
SUBTOTAL COSTS			$
COST OF MONEY	$	%	$
TOTAL COST			$
PROFIT/FEE	$	%	$
TOTAL PRICE/COST			$
GOVERNMENT SHARE, IF APPLICABLE			$
RECIPIENT SHARE, IF APPLICABLE			$

SUBCONTRACTORS/IOTs) & CONSULTANTS PRICE SUMMARY

A	B	C	D	E	F
SUB-CONTRACTOR IOT & CONSULTANT NAME	SOW TASKS PERFORMED*	TYPE OF AWARD	SUB-CONTRAC-TOR, IOT & CONSULT ANT	COST PROPOSED BY PRIME FOR SUBCONTRACTOR, IOT & CONSULTANT	DIFFERENCE (Column D - Column E) IF APPLICABLE
TOTALS					

*Identify Statement of Work, Milestone, or Work Breakdown Structure paragraph, or provide a narrative explanation as an addendum to this Table that describes the effort to be performed.

Appendix B.3 - Software and IP Costs

Software and IP Costs		
Item	**Cost**	**Date of Expiration**
(List)		

NOTE: Educational institutions and non-profit organizations as defined in FAR part 31.3 and 31.7, respectively, at the prime and subcontractor level may deviate from the cost template in Appendix B when estimating the direct labor portion of the proposal to allow for OMB guided accounting methods (2 CFR 220) that are used by their institutions. The methodology shall be clear and provide sufficient detail to substantiate proposed labor costs. For example, each labor category shall be listed separately; identify all Key Personnel and significant contributors provide hours/rates or salaries and percentage of time allocated to the project.

Appendix B.4 – Travel Costs Trip breakdown

		Trip Breakdown					
Base - Phase I:							
Trip #	Month of Trip	# of Travelers	Name of Traveler/Company	# of Days	Location	Purpose of Travel	Estimated Cost
Option Period - Phase II:							
Trip #	Month of Trip	# of Travelers	Name of Traveler/Company	# of Days	Location	Purpose of Travel	Estimated Cost
Option Period - Phase III:							
Trip #	Month of Trip	# of Travelers	Name of Traveler/Company	# of Days	Location	Purpose of Travel	Estimated Cost

Appenix B.5 – Contract Deliverables Table

Contract Deliverables				
SOW TASK#	Deliverable Title	Format	Due Date	Distribution/Copies
Continual	Monthly Contract Status Report	Gov't Format	10th of each month	Copy to PM, Contracting Officer and COTR
Continual	Monthly Technical Status Reports	Gov't Format	10th of each month	Standard Distribution**
** Standard Distribution: 1 copy of the transmittal letter without the deliverable to the Contracting Officer. 1 copy of the transmittal letter with the deliverable to the Primary PM and COTR.				