Broad Agency Announcement

Foundational Cyberwarfare (Plan X)

DARPA-BAA-13-02

November 20, 2012

Defense Advanced Research Projects Agency
675 North Randolph Street
Arlington, VA 22203-2114

Table of Contents

Part I: Overview

- **Federal Agency Name:** Defense Advanced Research Projects Agency (DARPA), Information Innovation Office (I2O)

- **Funding Opportunity Title:** Foundational Cyberwarfare (Plan X)

- **Announcement Type:** Initial Announcement

- **Funding Opportunity Number:** DARPA-BAA-13-02

- **Catalog of Federal Domestic Assistance Numbers (CFDA):** N/A

- **Dates**
    - Posting Date: See announcement at www.fbo.gov
    - Proposal Closing Date: January 25, 2013, 1200 noon (ET)
    - Proposers' Day Workshop was held October 15 and 16, 2012

- **Anticipated Individual Awards:** One award is anticipated in TA1 and TA5, and multiple awards are anticipated in TA2, TA3, and TA4.

- **Types of Instruments that May be Awarded:** Procurement contract or other transactions.

- **Technical POC**: Daniel Roelker, Program Manager, DARPA/I2O

- **BAA Email**: PlanX@darpa.mil

- **BAA Mailing Address For All Submissions**:
    - DARPA/I2O
      ATTN: DARPA-BAA-13-02
      675 North Randolph Street
      Arlington, VA 22203-2114

- **I2O Solicitation Website:** http://www.darpa.mil/Opportunities/Solicitations/I2O_Solicitations.aspx

Part II: Full Text of Announcement

I. FUNDING OPPORTUNITY DESCRIPTION

DARPA is soliciting innovative research proposals in the area of understanding, planning, and managing military cyber operations in real-time, large-scale, and dynamic network environments. Plan X will conduct novel research into the nature of cyberwarfare and support development of fundamental strategies needed to dominate the cyber battlespace. Proposed research should investigate innovative approaches that enable revolutionary advances in science, devices, or systems. Specifically excluded is research that primarily results in evolutionary improvements to the existing state of practice.

This broad agency announcement (BAA) is being issued, and any resultant selection will be made, using procedures under FAR Part 35.016. Any negotiations and/or awards will use procedures under FAR 15.4, Contract Pricing, as specified in the BAA. Proposals received as a result of this BAA shall be evaluated in accordance with evaluation criteria specified herein through a scientific review process.

DARPA BAAs are posted on the Federal Business Opportunities website (http://www.fbo.gov). The following information is for those wishing to respond to the BAA.

Background

Modern warfare requires militaries to rapidly plan, execute, and assess operations and campaigns across the full spectrum of conflict. The Department of Defense (DoD) has developed superior capabilities over decades in the physical domains of land, sea, air, and space. Cyberspace -- a collection of computer networks utilizing a variety of wired and wireless connections, a multitude of protocols, and devices ranging from super computers to embedded systems -- is emerging as a new warfighting domain. When called upon, the U.S. military must have equally superior capabilities to rapidly plan, execute, and assess the full spectrum of military operations in cyberspace.

The military is seeking to measure, quantify, and understand cyberspace. The military's current understanding and awareness in the cyber domain produces integration challenges with existing military capabilities in other domains. While existing technology can infer network topologies -- how computers are connected to one another -- using traceroute, packet analysis, and other techniques, the current research is just beginning to try to answer specific questions about the cyber domain. For example, where in a network topology should military platforms be deployed for a given mission? From which deployed units should capabilities be used to achieve mission objectives and in what sequence? Which routes through a network should be used in a network topology to optimize connection speed or robustness? What is the expected network path that data will take versus the actual path that data takes due to private and non-advertised routing agreements and tunnels?

Current technologies try to understand the cyber domain and answer these questions using a highly manual process with experts in the computer security and networking fields. In order to scale the number of operations, operational complexity, or compress the phases of reconnaissance, planning, and testing, additional computer security and network experts must be recruited and trained. This manual approach to military cyber operations is dependent on force size and skill. If an opponent's force is larger or more skilled, then the outcome is predictable. Militaries that rely on a manual approach must continually train more experts to stay head of opponents; however militaries that prioritize technology development can create a superior warfighting capability while maintaining a consistent force and skill level.

The manual approach also fails to address a fundamental principle of cyberspace: that it operates at machine speed, not human speed. In an environment where microseconds matter and operators use the keyboard to direct operations, the advantage goes to the opponent who can think and type faster. In the case of machine versus machine, the advantage goes to the hardware and software that executes faster. However, if an operator is technologically enabled to consistently outperform an opponent in all aspects of operational planning and execution in real-time, he would have a significant advantage.

Another challenge inherent in the manual approach is that commanders have few tools available to help them understand and quantify effects when considering whether to approve a plan. Exhaustive testing on cyber ranges may help gauge the potential effects of an operational plan, but such testing is time-intensive and not fully capable of modeling the dynamic nature of cyberspace. The actual cyber environment may have changed considerably from the test range environment by the time of mission execution. Further, if an operation requires any deviation from the plan during the course of execution, there is no time to retest on a range, leaving the commander uncertain of the effects of the deviation. The fundamental uncertainty and lack of flexibility inherent in the manual approach severely limits the utility of cyber capabilities for commanders.

In essence, the current manual approach has defined the way cyber operations are conceived and would be conducted – as asynchronous actions. Manual processes provide no capacity for real-time assessment and adjustment to adapt to changing battlespace conditions. The current paradigm is a simple progression of plan, execute, plan, execute, plan, execute . . . however if the process can be technologically optimized and the time-intensive requirements minimized, commanders will be able to leverage cyber capabilities in a more flexible manner, consistent with kinetic capabilities, to achieve real-time, synchronous effects in the cyber battlespace.

Defining the Plan X Cyber Battlespace

It is important to describe the conceptual cyber battlespace before outlining the Plan X program, since this is the environment the Plan X system will create, model, and present to military planners and operators. The Plan X definition of a cyber battlespace has three main concepts: 1) network map, 2) operational units, and 3) capability set.

At a high-level, the network map is a collection of nodes and edges and shows how computers are connected together. There are many ways to map a given network topology, including traceroute and packet analysis, as well as static architecture diagrams and dynamic routing protocol updates. The details of the network map depend on the type of network and protocols a specific network supports, including how often links between computers change and the properties of the links. There are two distinct layers of network map information: 1) logical topology and 2) meta-data.

The logical topology represents the direct connections between computers in a network and identifies which computers actively route packets to a destination. This definition leaves out passive network infrastructure, such as switches, hubs, and bridges, but does include network overlay topologies, such as encrypted tunnels, multiprotocol label switching, and private peering. A computer network's logical topology can be static or dynamic, and should represent the current logical topology as close to real-time as possible. For example, highly dynamic networks (e.g. mobile ad hoc networks), or an IP network that ignores or misrepresents common control message protocols, represent a difficult challenge in building real-time logical topologies. Given this potential for uncertainty, any network map will need to have this uncertainty quantified in different parts of the network map, or represent approximate logical topologies at some confidence level. Certain networks or parts of a network may be highly dynamic, while other parts may be static.

The second type of network information, meta-data, represents the specifics of each element in the logical topology. Recall that a logical topology consists of two types of elements, nodes and edges. Meta-data attaches properties to nodes and edges in the logical topology to create a property graph by using a variety of network and host reconnaissance techniques. Meta-data examples of an edge will include link capacity, latency, and persistence. Examples of node meta-data may include: number of links, operating system, patch level, protocols, ports, and other information currently identified using active and passive scanning techniques from common computer security tools.

Security infrastructure, such as firewalls, proxies, and intrusion detection/prevention systems, can be inferred by analyzing edge meta-data, when it is not an overt part of the network topology. For example, certain types of traffic or data may not pass through a given link, likely because of a silent filter or defensive technology. In this case, the logical topology can be updated to reflect silent but inferable active components.

Once a network map is created, it becomes the environment in which military planners and operators interact. A more comprehensive, higher-fidelity network map is better for operators and planners. However, sometimes planners and operators must maneuver in an uncertain environment just as our military forces do in physical domains.

Within this environment, military planners construct plans and deploy platforms, called operational units that use technology to conduct missions. Operational units and capabilities will differ depending on the type of cyber battlespace.

Operational units are deployed within the logical network topology. There are two primary types of operational units: 1) entry nodes and 2) support platforms.

An entry node provides the direct physical access into a network topology (i.e., this is the computer that an operator uses to direct and coordinate operations). Plans will typically include multiple entry nodes to increase the likelihood of mission success.

Support platforms are deployed in the cyber battlespace to control different aspects of an operation. This is similar to the various types of modern military aircraft: fighters, bombers, and unmanned aircraft, each designed to operate in and control a different aspect of air campaigns. Support platforms will enable similar functions in the cyber domain, including deploying capabilities, measuring collateral damage and conducting battle damage assessments, deploying defenses, and maintaining communications between entry nodes and support platforms.

Support platforms are deployed by 1) modifying an existing computer into a support platform, 2) using a preplaced, existing support platform, or 3) instantiating a support platform by extending or modifying the existing logical network topology. The main difference between a support platform and an entry node is whether a human is using it as an interface to access the cyber battlespace. If a human is directly using it, then it is an entry node.

The capability set is the collection of technologies that a military can use to affect and control a given cyber battlespace. These technologies can be broadly defined in three categories: 1) access, 2) functional, and 3) communication.

Access technologies allow a planner to execute arbitrary instructions on a computer. In common terms, this is an exploit that can be used to run programs or payloads. In military planning terms, this technology is an enabler and will most commonly be used to turn an existing computer into a support platform, or to execute either a functional or communication technology to achieve the mission objectives.

Functional technology represents all the other types of technology that affect computers and networks. For example, rootkits, keyloggers, network scanners, denial-of-service, defense evasion, network/host reconnaissance, operating system control, and effect measurement. The larger the functional technology set a military planner can leverage, a larger variety of plans can be developed by combining functional components.

Communication technology provides a way for entry nodes, support platforms, and system capabilities to exchange information. Examples of this type of technology include malware command and control methods, such as DNS, peer-to-peer, and HTTP SSL connections. Each technique has unique capabilities in terms of channel detection, max bit rate, and latency. It is important to note that depending on the communication technology that a military planner uses, the plan may have inherent limitations in terms of timing, sequencing, and the amount of data communicated between nodes.

Program Scope

The Plan X program seeks to build an end-to-end system that enables the military to understand, plan, and manage cyberwarfare in real-time, large-scale, and dynamic network environments. Specifically, the Plan X program seeks to integrate the cyber battlespace concepts of the network map, operational unit, and capability set in the planning, execution, and measurement phases of military cyber operations. To achieve this goal, the Plan X system will be developed as an *open platform architecture* for integration with government and industry technologies.

The Plan X program is *explicitly not funding* research and development efforts in cyberweapon-related technologies such as vulnerability analysis, command and control protocols, or end effects.

Plan X is planning to fund the following five technical areas (TA) to build a prototype system:

- TA1 - System Architecture. The System Architecture team will build the Plan X system infrastructure and support overall system design and development. This includes secure architecture design, development of application programming interfaces (APIs), and data format specifications. The System Architecture team will also be responsible for purchasing system hardware and maintaining the overall infrastructure. The Plan X system should support external connectivity to performer locations and be able to be certified and accredited utilizing the Intelligence Community Directive Number 503 (ICD 503), "Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation."

- TA2 - Cyber Battlespace Analytics. Performers in this area will develop automated analysis techniques to assist human understanding of the cyber battlespace, support development of cyberwarfare strategies, and measure and model battle damage assessment. Data sets will include logical network topologies, and node / link attributes.

- TA3 - Mission Construction. Performers in this area will develop technologies to construct mission plans and automatically synthesize plans to an executable mission script. Performers will also develop technologies to formally verify plans and quantify the expected effects and outcomes. TA3 involves the development of cyberwarfare domain specific languages, program synthesis, and automated program construction from high-level specifications.

- TA4 - Mission Execution. Performers will research and develop: 1) the mission script runtime environment and 2) support platforms. The runtime environment will execute mission scripts end-to-end, including construction of capabilities and support platform deployment. The support platform research area focuses on building operating systems and virtual machines designed to operate in highly dynamic and hostile network environments. Support platforms will be developed to operate on all computer architecture levels, from hypervisor to sandboxed user applications.

- TA5 - Intuitive Interfaces. The Intuitive Interfaces team will design the overall Plan X user experience, including workflows, intuitive views, motion studies, and integrated visual applications. Coordinated views of the cyber battlespace will provide cyberwarfare functions of planning, execution, situational awareness, and simulation.

Performers will work closely with all other technical areas to ensure that the needed graphical user interface (GUI) APIs are defined and provided.

The Plan X program is structured around an on-site Collaborative Research Space (CRS), located in Arlington, VA, where performers will be organized as a virtual technology startup. Performers will be expected to conduct research and development at off-site facilities. However, key integration personnel will be staffed at the CRS where all technologies will be integrated, revision controlled, and tested. Each performer in TA1 through TA5 must staff 1-2 integration experts at the CRS. The CRS will be accredited as a Collateral Secret area and personnel staffing the CRS must possess a Secret security clearance.

Proposers interested in the System Architecture technical area (TA1) should highlight expertise in building and supporting large-scale, highly interactive systems using advanced GUIs. TA1 proposers should also address rapid acquisition processes for required system hardware and software. No more than one System Architecture performer will be selected.

Proposers interested in TA2 through TA5 should identify and describe the specific technology being built, how it fulfills the requirements of the technical area, and most importantly, how it will provide capability and integrate with the end-to-end Plan X system. It is important to note that no technology will be delivered as a stand-alone product. All technology will be integrated into the full system located at the CRS. Proposals should specifically address how developed technology will fit into the whole end-to-end system, including notional ideas of the required data inputs, outputs, and API structures to operate.

Technical Areas

The Plan X program and its technical areas will build a system that can create, model, simulate, and control a cyber battlespace in real-time. However, the Plan X program will not fund all the technical areas required to achieve this vision, because many technical areas can be directly leveraged from other sources, such as the public domain or from existing DoD technology. The Technical Area section will specifically address which technologies will be funded as part of Plan X and which technologies will not be funded. **Performers must understand that proposed technologies that fall outside of the described Plan X technical areas will not be evaluated.**

Specific technologies that will not be funded under Plan X include active and passive mapping techniques and capability set technology (e.g., access, functional and communication technologies).

Technical Area 1: System Architecture

There are two primary foci of the System Architecture team: 1) the design and implementation of the cyber battlespace graphing engine, and 2) the design and integration of the end-to-end Plan X system.

The cyber battlespace graphing engine is the core of the Plan X system. The graphing engine's primary task is to receive, store, model, retrieve, and send cyber battlespace information to other Plan X system components. The graphing engine receives real-time information from various network mapping components and operational overlay sources. This information will represent a majority of the overall information that the graphing engine receives, and is comprised of the data set that the graphing engine uses to create the cyber battlespace. All other components of Plan X will interact with this created model.

The network mapping components send data that allow the graphing engine to convert and construct a real-time logical network topology. This information will include traceroute data, link latencies, BGP routes, IP Time-To-Live (TTL) header analysis, node routing tables, and any other type of information necessary to assist in constructing the logical network topology. The Plan X system must be able to model network topologies at Internet-level scales. Proposers should consider how to optimally build, store, and update network topologies of various sizes and protocols (including non-IP networks) in real-time.

Operational execution overlay information is stored as meta-data for each element in the logical network topology. For example, operational overlay information will include the operating system identification, network service profile, defensive and offensive capabilities, and identification, friend or foe (IFF). Providing this overlay information requires the graphing engine to allow logical network topology elements to be easily extensible.

The planning and operational areas will attach another layer of information on top of this constructed cyber battlespace model. Planning information includes the potential entry nodes, support platform placement, communication paths, and target sets. Planners will be able to checkpoint plans under development so that the current plan state is available for commanders and other planners to analyze and modify. Operational execution information will include the real-time status as an operation unfolds, including the state of entry nodes, support platforms, battle damage assessment, measured effects, and capability status.

Centralizing operational planning and execution status will allow the Plan X system to show a global heat map of its activities, from conceptual to actual. This capability allows planners to have a more global view of ongoing activities, which may impact the plan being developed. For example, if an entry node is being overused in either ongoing operations or developing plans, then a planner may want to select another entry node. Viewable information is controlled by access control tags and should be extensible, supporting broad classes of information down to specific operational phases and actions.

The second focus of TA1 is to design and build the end-to-end Plan X system infrastructure. This includes the required staff necessary to design, operate, and maintain the Plan X development and test infrastructure. The TA1 team will also provide the necessary administration to include security certification and accreditation for the Plan X system. The design will be developed in collaboration with government partners and other technical area performers to ensure the system can support required technology integration points and functional military planning and operational requirements.

The TA1 team should address secure software architecture design principles in the Plan X system. Additionally, proposers should notionally address how the Plan X system could operate from Unclassified to Top Secret / Special Compartmented Information / Special Access Program with the possibility of multiple simultaneous technology evaluations operating at different security levels and compartments.

There will be many design iterations during the course of the four-year program, resulting in a standardized architecture; however, proposers should consider, explain, and evaluate different approaches to provide a basis of confidence in their proposed solution. This includes both the software architecture and estimated hardware requirements.

The TA1 team is not responsible for other components, but will support overall integration efforts. The TA1 team is responsible for creating and maintaining system architecture diagrams, APIs, data structures, and object definitions, including requirements to integrate third-party technology.

Proposers are encouraged to analyze and compare existing commercial real-time, simultaneous system architectures, like engine architectures used in large-scale gaming environments. In particular, proposers should consider the potential architecture similarities of real-time updates, multi-user interface, event modeling, API structure, and simultaneous transactions.

TA1 proposers should also address specific large-scale graph processing architectures, including memory-based implementation and cluster-based implementations. Memory-based graph processing is feasible depending on how Internet-scale battlespaces are partitioned. Cluster-based implementations using Apache Giraph, Aurelius's Titan, and other approaches are inherently scalable depending on the graph optimizations and structures being processed. Proposers should consider the tradeoffs between both approaches, including scalability and processing time.

It is important to note that the TA1 team will work directly with the Cyber Battlespace Analytics (TA2) performers to ensure that the cyber battlespace graphing engine will support the developed TA2 modeling approaches and algorithms.

Technical Area 2: Cyber Battlespace Analytics

The primary focus of the Cyber Battlespace Analytics technical area is to model, reason, and assist military planners to navigate and build strategically sound and tactically feasible cyber operations. There are two research areas within TA2: 1) development of automated techniques to assist military planners to construct cyberwarfare plans, and 2) support of wargaming applications, such as modeling opponent moves and counter moves, to optimize planning. TA2 performers will use the data residing in the System Architecture technical area (TA1) cyber battlespace graphing engine to develop approaches and algorithms to assist planners in developing plans. TA2 is critical in achieving the full Plan X vision, as the speed of planning hinges on using machine assistance to automate as much of the process as possible.

There are many common phases to developing cyberwarfare plans across a wide variety of scenarios within a cyber battlespace. TA2 will work directly with cyber operations planners and the Intuitive Interface technical area (TA5) to help develop efficient planning processes, identify areas for automation and machine assistance, and integrate directly with the planning process.

An important part of TA2 is to understand and quantify cyber battlespace effects. Proposers should address the type of information that is needed to analyze and model planned effects. This may include network effects at macro and micro levels, node effects, and combined network and node models to assess any resulting collateral damage. This area may require different approaches and information that is not contained in the cyber battlespace graphing engine. Performers should address why these approaches are needed and how they will be integrated into the Plan X system. Proposers should consider a wide range of approaches that can support different probabilities of certainty to measure cyber battlespace effects and overall collateral damage.

Anticipated research opportunities in automating planning processes might include, but are not limited to:

- *Node selection*. Planners will need assistance selecting optimal nodes in a cyber battlespace. Node sets might include entry nodes, target nodes, and nodes to avoid. Selection will likely occur based on a set of properties stored in the System Architecture technical area (TA1) cyber battlespace graphing engine, with planners visually inspecting the selected node set in a typical network topology overlay. Node selection may also be contingent not just on specific properties but also on relational properties within the battlespace graph, such as hops to other nodes, overall latency to another node set, or connectivity to a particular sub-graph within the cyber battlespace.

- *Topology reduction*. Given an entry node set and a target node set, a reduction of the overall topology being reasoned over to a mission topology subset is possible using a combination of common path selection algorithms, such as shortest path, minimum diameter, or maximum latency may be beneficial. This reduction allows succeeding algorithms to run significantly faster. It should be noted that reduced topologies might need to be incrementally expanded, depending on the specific objectives of a mission.

- *Support platform placement*. Given a reduced network topology, including an entry node set and target node set, proposers should determine the optimal location and number of support platforms needed to achieve a mission’s goals. Developed algorithms will consider network topology data along with any operational overlay data, to determine the optimal location and number. Analyses including: 1) cost-benefit calculation of the cost to deploy support platforms to nodes using access technologies, and 2) optimal placement in regard to latency speed, path number to target nodes, and connectivity to entry nodes in order to maintain positive control. Developing and analyzing additional calculations is strongly encouraged in TA2 proposals.

- *Communication path selection*. It is infeasible for human operators to identify and maintain network paths between entry nodes, support platforms, and target nodes during both planning and operational execution. Identified network paths between components are not only dictated by default routing. Paths will likely be constructed as an overlay on existing network topology physical links, as in commercial content delivery networks (CDNs). Automated techniques should be developed that can establish primary and alternate routes between planning components, based on a set of attributes, including: 1) number of communication nodes required to establish a route, 2) overall latency between components, 3) paths excluding a specified node set, and 4) maximum link bandwidth. Developed algorithms should consider that topologies change in real-time and identified paths will need to be continuously updated based on the specified path attributes.

TA2 proposers are *strongly encouraged* to develop and analyze additional opportunities to demonstrate an understanding of the first research topic (i.e. development of automated techniques to assist military planners in constructing cyberwarfare plans).

The second research topic within TA2 is the development of cyberwargaming techniques to analyze potential adversarial dynamics and simulate and evaluate operational plans as they are being developed. While the goal of the first TA2 topic area is to assist planners to develop plans that achieve mission goals, the objective of the second TA2 topic area is to create plans that are robust in reflecting the dynamic nature of the cyber battlespace and the ability to measure and achieve mission goals in the face of active opposition. Approaches may include detailed computer-simulated opponents, human opponents, or random events that impact the cyber battlespace or resources available for operational planning.

Specifically, TA2 proposers should describe how they plan to investigate approaches to model potential opponent moves and counter moves during plan construction. This may include simulating potential opponent strategies and tactics against a defined opponent model. Approaches may involve the simulation of the developed mission plan using network simulation and modeling technology, and testing plans against common plan weaknesses or random events. This approach could be compared to techniques used in evaluating software for common bug classes or random and targeted fuzzing to uncover potential weaknesses in software. TA2 proposers are *strongly encouraged* to develop and analyze additional opportunities to demonstrate an understanding of the cyberwargaming topic area.

TA2 proposals may address a single topic area or both topic areas. Proposers should describe how algorithms and techniques will be integrated into the Plan X system. Assumptions such as data input/output or system requirements should be specifically identified and addressed.

Technical Area 3: Mission Construction

The goal of the Mission Construction technical area (TA3) is to develop automated techniques that allow mission planners to graphically construct detailed and robust plans that can be automatically synthesized into an executable mission script. Because research and technologies developed in TA3 will directly support the Intuitive Interfaces technical area (TA5), proposals should specifically address how the proposed technology will integrate and enable TA5 development.

The overall approach to achieving TA3 objectives leverages the inherent nature and structure of a cyberwarfare mission. Central to this structure is the network topology for which an operation is planned. In the case of computer networks, the network topology or graph is inherently undirected. When overlaid with a data set for a given operation, the overlaid network topology becomes a directed graph by including: 1) the paths connecting nodes and the sequence in which they are established, 2) the specific instructions, logic, and events executed at each node, and 3) the sequential branches resulting from node processing.

Intuitively, this structure begins to represent a program control flow graph (CFG). Instructions executed at a node, whether an entry node, support platform, or target node, may transfer program control by "calling" other nodes as the mission progresses. Called nodes execute instructions, returning the calculation results to either the calling node or a central coordination node. A mission program may terminate by either achieving a specific goal or affecting the cyber battlespace in a specific way for a specific duration.

Understanding this concept and investigating the structure of cyberwarfare program CFGs is a critical TA3 research topic. Cyberwarfare program CFGs and programming paradigms may resemble many different types, including single threaded, multi-threaded, distributed, concurrent and parallel computing designs. TA3 proposers are encouraged to evaluate and develop domain specific languages (DSLs) to plan and execute cyberwarfare missions using various elements from the previous analysis of programming and computing designs. Mission Construction proposals should also describe how a developed cyberwarfare DSL will integrate and support TA5 and developed GUIs.

Other aspects to consider in developing a cyberwarfare DSL include, but are not limited to:

- *Operation checkpointing*. Allow planners to build in "checkpoints" during mission execution for real-time operator interaction. Plans may ask an operator to choose sequential actions, provide additional information, or upload courses of action.

- *Real-time failover*. DSLs need to support the ability to allow manual real-time operator control. Failover must be graceful and efficient, allowing an operator to rapidly direct and control all aspects of an ongoing mission. Real-time failover capability development will include collaboration with the Intuitive Interface technical area (TA5).

- *Levels of autonomous operation*. DSL technology should address how and to what extent mission program logic is able to operate autonomously if communications are lost or degraded. Planners must explicitly mark instructions and actions that could be autonomously executed without operator monitoring or status.

- *Formal analysis*. By translating mission plans into program CFG structures, TA3 research can leverage many existing techniques and technologies in program analysis and formal methods. This allows translated plans to be evaluated for errors, bugs, and inconsistencies. Additionally, these techniques can be used to prove and enforce collateral damage measurements and actions. For example, formal analysis can guarantee that execution is stopped if certain collateral damage parameters or thresholds are exceeded.

- *Enforcing Rules of Engagement (ROE)*. Plans should be constructed to programmatically limit and enforce operator options and actions, according to a commander's specified ROEs. By integrating ROEs directly into a plan, they can be seamlessly integrated into a mission script during the script synthesis process. This allows formal analysis techniques to mathematically prove the limitations of an operator's ability to negatively affect the mission and operate without authority.

- *Cyber operation "play book"*. Planners may develop specific and unique "plays" to assist in planning future missions. This concept is similar to a football playbook that contains specific plays developed for specific scenarios. The cyberwarfare DSL should be able to capture and store developed "plays" and collaborate with TA2 performers to ensure that the "play" can be applied and adapted to specific network topologies.

Once a cyberwarfare mission plan is represented in a programmatic CFG, the next step is to compile or synthesize the plan into a fully encapsulated executable program or script. This includes the generation and deployment of the required capability sets and the required instantiations of support platforms.

The output of the mission synthesis is to compile a fully operational mission package to deliver to the Mission Execution technical area (TA4). The mission synthesis process should support the ability to directly include an executable capability set in the case of missions involving networks without direct access to required repositories. The output of TA3 is a fully operational mission package that includes all the logic to completely deploy and execute all aspects of the mission plan, including specific instantiations of instruction sets to be executed at each support platform. The mission package should also include the mission script, ROE access control lists, and the capability set specification for TA4 teams to assemble. Approaches should assume that support platform and capability set technology will not be delivered as part of the operational package, but instead be deployed from distributed locations.

TA3 proposals should show how program synthesis and automatic program construction from high-level specifications could be applied to achieve the mission synthesis goal. Other approaches may be feasible and proposers should address why and how another mission synthesis approach is better. TA3 proposals and deliverables that do not address all TA3 research topics (i.e. plan development and program synthesis) may be evaluated as weak and have a lesser chance of being selected.

Technical Area 4: Mission Execution

The Mission Execution technical area focuses on research and development in two research topics: 1) the mission script runtime environment and 2) support platforms. TA4 proposals may address either or both topic areas. The goal of TA4 is to receive an operational package from the Mission Construction technical area (TA3) and seamlessly execute it, while providing real-time status and operator control through the Intuitive Interface technical area (TA5).

The mission script runtime environment is central to achieving the Plan X vision, controlling the entire execution of a mission, and supporting real-time operator interaction. The runtime environment can execute a TA3 mission program, which may include assembling required capability technologies, deploying support platforms, uploading TA3 mission program instruction blocks to support platforms, and enforcing ROE access control lists.

Depending on the specific program language implementation of TA3, the TA4 runtime environment should be able to leverage multiple aspects of existing program language runtimes during the design and development process. Proposers should investigate and discuss in the runtime approaches and strategies to support their unique technical approach in the proposal.

TA4 proposers should leverage public and commercial capabilities such as Metasploit, Immunity CANVAS, and other standard toolkits as representative technology sets. The TA4 runtime environment will use these standard toolkits to build an extensible API framework for assembling capabilities for each mission program. This approach allows the capability assembly process to integrate with multiple technology repositories and support future requirements.

The design and development of the TA4 runtime will involve close collaboration with TA3 performers and will be developed in tandem with the TA3 cyberwarfare DSL and mission synthesis technologies. TA4 proposals should highlight the team members' experience and expertise in developing exploitation "throwing" frameworks, penetration testing tools, capability development, and other operational technology development. Proposals in this area will be evaluated based on the runtime development approach, domain analysis, and prior team member experience in developing similar systems.

The second research topic, support platforms, focuses on the development of operating systems and virtual machines designed to execute cyberwarfare missions in highly dynamic and hostile cyber battlespaces. Just like militaries have various vehicles designed to perform specific warfare functions, like tanks, unmanned vehicles, bombers, fighters, aircraft carriers, etc., militaries also need specialized platforms that provide specific cyberwarfare functions. Notional support platforms might include, but are not limited to:

- *Launch platforms*. These platforms support operational functions such as active capability deployment, front-line position, multiple simultaneous mission execution, and intrusion containment.

- *Battle effect monitor*. This platform supports operational functions like passive and active mission effect measurement, status of deployed support platforms, integrity of mission communications to identify tampering, and other analytic functions.

- *Communication relay*. These platforms support the establishment of mission-specified routes through a given network topology. The platform should support multiple types of communication protocols, latency, and bandwidth requirements.

- *Adaptive defense*. These platforms support defensive functions like filtering packets and connections, notifying other support platforms of detected attackers, deploying capability antidotes to mitigate both previously deployed capabilities and detected adversary capabilities.

TA4 proposers are ***strongly encouraged*** to develop and address additional platform types to demonstrate a thorough understanding of the cyber platforms topic area.

Approaches may leverage a common platform base with specific modules supporting the various platform functions. Technologies such as virtual machines, hypervisors, correct-by-construction microkernels, application sandboxing, and domain isolation may be directly applicable. Platforms should also support multiple installation forms so that they can be deployed at all computer architecture levels that may be encountered. This includes the hypervisor, kernel, and user levels of an operating system.

The developed platforms are expected to work on a set of performer-selected architectures and operating systems to demonstrate feasibility and proof-of-concept. Support platforms are expected to be installable on commodity computer architectures and should not require specialized hardware to operate.

Technical Area 5: Intuitive Interfaces

The goal of the Intuitive Interface technical area (TA5) is to provide a fully integrated visual user experience for commanders, planners, and operators to manage cyberwarfare activities. All other technical areas will directly support TA5 to develop and provide the best user experience possible. Since it is anticipated that one performer will be selected in TA5, proposers should address all aspects of user experience, including user profiles, design, workflow modeling, motion studies, color palettes, and GUI development. TA5 proposals will likely require a large team, in particular, those with commercial user experience and design companies, to provide the required depth and breadth of capability and expertise.

TA5 proposers are encouraged to adopt and leverage commercial user experience standards to design and develop GUIs and data workflows. Many aspects of the Plan X vision use similar concepts and architecture principles found in large-scale gaming platforms. Since one of the primary goals of TA5 is to minimize the required technical expertise for commanders, planners, and operators, leveraging game development concepts and design should allow for maximum user engagement. For example, progressing from beginner to advanced levels can assist rapid user training and proficiency.

The technical and system architecture similarities of large-scale gaming platforms when compared to the Plan X system are also worth noting. These large-scale platforms model a cyber battlespace environment and update this environment in real-time while supporting millions of users actions simultaneously. Similarly, Plan X will model the cyber battlespace and update it with incoming mapping, operational status, and planning information from potentially millions of users.

TA5 will develop four integrated graphical interface workflows to allow users to interact and control various Plan X functions:

- *Real-time cyber battlespace views*. The workflow and views associated with this graphical interface are focused on visualizing large-scale cyber battlespace activity levels. In essence, this is the heat map of all ongoing operations, plans in development, and real-time structure of network topologies. This battlespace view must support data filtering capabilities so that commanders can quickly zoom in and view a specific ongoing operation or a plan in development. This workflow should also support an unencumbered cyber battlespace view that does not include any operational status, planning, or other Plan X overlays.

- *Planning process*. The planning process workflow and view development is potentially the most critical and complex of all four TA5 views. TA5 proposals should address how the planning process workflow will be developed during the course of the program and include notional workflows to demonstrate an understanding of this area. These workflows may range from extremely hierarchical to massively crowdsourced approaches. TA5 proposals should also address how plans are assembled. The assembly process might include network topology reductions, node selection, presentation of meta-data associated with the area-of-operation, goal measurements, and alternate actions. Developed plans must include alternate contingency plans to ensure that mission goals will be achieved. In an environment where microseconds matter, going back to the drawing board after a mission failure is likely to result in defeat.

- *Capability construction*. The overall planning process should address the construction of the specific capabilities that will be used during the course of a mission. While certain capabilities are easily derived from data stored in the cyber battlespace graphing engine, specific mission effects may need to be constructed. Capability set construction will rely on the assembly of a set of components based on their effect attributes, allowing the operator to mix and match components in order to adapt to various mission requirements.

- *Operator controls*. The operator control workflow should support two sub-workflows. The first workflow should focus on operational package execution and provide operator interaction with the mission script. The second workflow should focus on real-time operator interaction without a mission script. This second workflow is to support real-time engagements that may occur without the possibility for plan creation. As such, the real-time interaction may be a combination of on-the-fly planning with direct feedback. Operator control views should capture the singular focus of an operator’s mindset and significantly reduce operator decision reaction time.

TA5 proposers are encouraged to develop and address additional graphical interface workflows and views if they think it is necessary to achieve the Plan X vision.

All workflows and views developed in TA5 should produce a unified representation. TA5 should leverage look and feel commonalities between each workflow and view so that planner and operator roles are easily interchangeable.

TA5 approaches will likely leverage commercial user experience standards to design and develop GUIs and data workflows. Proposals should also address notional API specifications for each view to illustrate an overall understanding and integration with the Plan X system.

The graphical interfaces developed during the course of the program will be designed to allow a variety of user input and display devices. Touch interface technologies, tablet computing, and augmented reality displays, should be taken into consideration in the design and development of the user interface and user experience of Plan X. Traditional keyboard/mouse interactions are anticipated but should be minimized. Proposers should explicitly describe the combined team's experience with touch interface technologies by listing previously developed touch interface applications and the success of such technologies within the commercial space, including the Android Marketplace and iTunes Appstore.

Program Structure

The Plan X program is structured around the on-site CRS where performers will continuously integrate developing technologies into the end-to-end Plan X system. Performers are expected to have off-site development facilities, accredited in accordance with the level of classified work they may be performing, as applicable. Performers should plan on providing 1-2 full-time expert integration software developers at the CRS. When selecting these candidates, performers should consider team dynamics since the on-site personnel will work closely together, operating as a single team.

The Plan X program will maintain the CRS in Arlington, VA, to facilitate agile and collaborative software development. User interaction, use-case development, system integration, testing, and evaluation are all intended to take place at the CRS. DARPA intends to arrange program interaction with a variety of users from DoD and other government agencies, including on-site military personnel who will be testing and using the Plan X system on a daily basis. Performers should include in the proposal the hardware and software costs necessary for staffing the 1-2 personnel at the CRS. Each performer should support their own off-site facilities as well as their off-site hardware and software requirements.

Plan X will follow agile methodologies using two-week, sprint schedules. Proposals must reflect this approach and describe the first twelve sprints up to the delivery of the alpha release of the end-to-end system at 6 months. Performers will be expected to check in code to the central Plan X code repository continuously.

Proposals will be evaluated on the experience and strength of the team, including the past work that each individual has contributed to the technical area. In order to provide the strongest team possible, performers are strongly encouraged to combine current employees, unique commercial companies, and expert industry consultants. Resumes are required for each team member, highlighting past technical contributions and experience in high performance software development teams (see Appendix B).

Interested proposers will specifically address how proposed technology will integrate into the full Plan X system, including the notional APIs that the Plan X system would need to provide.

This includes describing the overall integration approach. Proposers should not address how the proposed technology could be a stand-alone product, since full system integration is the Plan X goal.

Schedule and Milestones

The Plan X program is designed to run for four (4) one-year phases and follows a rigorous product release schedule. Each phase consists of four (4) development spirals, which includes six (6) two-week development sprints ending in a one-week design checkpoint. The design checkpoint will include reviewing the previous development spiral activities and planning the next development spiral. Design checkpoints will replace the standard interim progress review (IPR) events normally held as part of program schedules.

Each phase will consist of one major milestone and four minor milestones. The major milestone, the Plan X product launch, occurs at the end of each phase. The Plan X product launch will be a two-day event that is open to both government and industry, and will showcase the Plan X system and technology that was developed over the previous phase.

The first day of the product launch will consist of technical briefings and discussions in the morning, with the afternoon focused on attendees using and testing the Plan X system. The second day is a mini-developer conference where the Plan X development team will explain how to use and interface cyberwarfare technologies with the Plan X system and Plan X software development kits (SDKs). The purpose of the second day is to foster and build a broad Plan X developer community in government and industry. This will allow DARPA to evaluate new technologies for future funding opportunities, support government partners integrating existing technologies, and test the “open platform” architecture of the Plan X system.

Proposed schedules will include a six-week ramp up period (three (3) two-week sprints) leading up to the Phase I kickoff. This ramp up period is to prepare the CRS for the program start and design the first development spiral for Phase I. System Architecture technical area (TA1) proposals will scope this ramp up period to include the full team to support acquisition and deployment of system architectures and the CRS infrastructure. TA2 through TA5 proposals will scope this ramp up period to include the Principle Investigator and the on-site integration lead to support the design of the first development spiral.

All proposals should include costs to support four one-week design checkpoints per phase. This will include off-site team member lodging and travel to DARPA for the event. All proposals should include a base performance period of 12 months (Phase I) with three 12-month options (Phases II, III and IV).

If proposers address specific objective metrics for the fully integrated technology capability, then the objectives should be protected at the collateral SECRET level in accordance with the Plan X Security Classification Guide (SCG). See Section IV.A on how to obtain a copy of the Plan X SCG.

Deliverables

All performers shall be required to provide the following deliverables:

- *Slide Presentations*. Performers will deliver presentations after technical meetings and have up to one month after meetings to annotate or add information to the slides presented before final submission to the government.

- *Source Code and System Documentation*. System documentation shall be provided within one month after the end of each phase, documenting the source code, hardware description, language specifications, system diagrams, part numbers, and any other data necessary to replicate and test technology developed on the program. Source code will be checked in daily.

- *Monthly Progress Reports*. Progress report should address technical progress made and any issues requiring the attention of the government team. Reports should also provide financial status by showing total contract award, total funded, planned expenditures by month and actual expenditures by month as well as a list of personnel working on the effort each month. Monthly progress reports will be a maximum of two pages.

- *Final Report*. Required by the end of contract performance. Final report will address technical progress and future recommendations of the technology area. The final report has a maximum of five pages.

- Reporting as necessary and described in Section VI.

II. AWARD INFORMATION

Multiple awards are anticipated. The level of funding for individual awards made under this BAA has not been predetermined and will depend on the quality of the proposals received and the availability of funds. Awards will be made to proposers whose proposals are determined to be the most advantageous and provide the best value to the Government, all factors considered, including the potential contributions of the proposed work, overall funding strategy, and availability of funding for the effort. See Section V.B for further information.

Proposals selected for award negotiation may result in a procurement contract depending upon the nature of the work proposed, the required degree of interaction between parties, and other factors. In all cases, the DARPA contracting officer shall have sole discretion to select award instrument type and to negotiate all instrument provisions with selectees.

As of the date of publication of this BAA, DARPA expects that program goals for this BAA may not be met by proposers intending to solely perform "fundamental research," as defined by National Security Decision Directive 189.[1] Therefore, DARPA anticipates restrictions on the resultant research. Notwithstanding this statement of expectation, DARPA recognizes that proposed research solutions could be of either a fundamental or restricted nature. Proposers should indicate in their proposal whether they believe the scope of the research included in their proposal is fundamental or restricted, with the understanding that in all cases, the DARPA contracting officer shall have sole discretion to select award instrument type and to negotiate all instrument provisions with selectees. See Section VI.B.5 for further information on fundamental, non-fundamental, and restricted research.

The Government reserves the right to:

- Select for negotiation all, some, one, or none of the proposals received in response to this solicitation.
- Make awards without discussions with proposers.
- Conduct discussions if it is later determined to be necessary.
- Segregate portions of resulting awards into pre-priced options.
- Accept proposals in their entirety or to select only portions of proposals for award.
- Fund proposals in phases with options for continued work at the end of one or more phases.

[1] "Fundamental research means basic and applied research performed [on campus] in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community, as distinguished from proprietary research and from industrial development, design, production, and product utilization, the results of which ordinarily are restricted for proprietary or national security reasons."

- Request additional documentation once the award instrument has been determined; such information may include but is not limited to representations and certifications.

- Remove proposers from award consideration should the parties fail to reach agreement on award terms within a reasonable time or the proposer fails to provide requested additional information in a timely manner.

III. ELIGIBILITY

A. Applicants

All responsible sources capable of satisfying the Government's needs may submit a proposal that shall be considered by DARPA.

1. Historically Black Colleges and Universities (HBCUs), Small Businesses, Small Disadvantaged Businesses and Minority Institutions (MIs)

HBCUs, small businesses, small disadvantaged businesses and MIs are encouraged to submit proposals and team with others to submit proposals; however, no portion of this announcement will be set aside for these organizations due to the impracticality of reserving discrete or severable areas of this research for exclusive competition among these entities.

2. Federally Funded Research and Development Centers (FFRDCs) and Government Entities

FFRDCs and Government entities (e.g., Government/national laboratories and military educational institutions) are subject to applicable direct competition limitations and cannot propose to this BAA in any capacity unless the following conditions are met.

- FFRDCs must clearly demonstrate that the proposed work is not otherwise available from the private sector and must provide a letter on letterhead from their sponsoring organization citing the specific authority establishing eligibility to propose to Government solicitations and compete with industry, and compliance with the associated FFRDC sponsor agreement and terms and conditions. This information is required for FFRDCs proposing as either prime contractors or subcontractors.

- Government entities must clearly demonstrate that the proposed work is not otherwise available from the private sector and provide documentation citing the specific statutory authority (and contractual authority, if relevant) establishing their eligibility to propose to Government solicitations.

At the present time, DARPA does not consider 15 U.S.C. § 3710a to be sufficient legal authority to show eligibility. While 10 U.S.C. § 2539b may be the appropriate statutory starting point for some entities, specific supporting regulatory guidance, together with evidence of agency approval, will still be required to fully establish eligibility.

DARPA will consider eligibility submissions on a case-by-case basis; however, the burden to prove eligibility for all team members rests solely with the proposer.

3. Foreign Participation

Non-U.S. organizations and/or individuals will not be afforded access to classified aspects of Plan X, but may participate to the extent that such participants comply with any necessary nondisclosure agreements, security regulations, export control laws, and other governing statutes applicable under the circumstances.

B. Procurement Integrity, Standards of Conduct, Ethical Considerations and Organizational Conflicts of Interest

Current Federal employees are prohibited from participating in particular matters involving conflicting financial, employment, and representational interests (18 U.S.C. §§ 203, 205, and 208). Prior to the start of proposal evaluation, the Government will assess potential conflicts of interest and will promptly notify the proposer if any appear to exist. The Government assessment does not affect, offset, or mitigate the proposer's responsibility to give full notice and planned mitigation for all potential organizational conflicts, as discussed below.

In accordance with Federal Acquisition Regulation (FAR)[2] 9.503 and without prior approval or a waiver from the DARPA Director, a contractor cannot simultaneously be a scientific, engineering, and technical assistance (SETA) contractor and a performer. As part of the proposal submission, all members of a proposed team (prime proposers, proposed subcontractors and consultants) must affirm whether they (individuals and organizations) are providing SETA or similar support to any DARPA technical office(s) through an active contract or subcontract. Affirmations must state which office(s) the proposer and/or proposed subcontractor/consultant supports and must provide prime contract numbers. All facts relevant to the existence or potential existence of organizational conflicts of interest (FAR 9.5) must be disclosed. The disclosure shall include a description of the action the proposer has taken or proposes to take to avoid, neutralize, or mitigate such conflict. If, in the sole opinion of the Government after full consideration of the circumstances, a proposal fails to fully disclose potential conflicts of interest and/or any identified conflict situation cannot be effectively mitigated, the proposal will be rejected without technical evaluation and withdrawn from further consideration for award.

If a prospective proposer believes a conflict of interest exists or may exist (whether organizational or otherwise) or has a question as to what constitutes a conflict, a summary of the potential conflict should be sent to PlanX@darpa.mil before preparing a proposal and mitigation plan.

C. Cost Sharing/Matching

Cost sharing is not required; however, it will be carefully considered where there is an applicable statutory condition relating to the selected funding instrument (e.g., other transactions under the authority of 10 U.S.C. § 2371). See Section IV.B.2.e for further information on cost sharing requirements for other transactions.

1. Submission of Proposals to Multiple Technical Areas

Proposers may submit proposals for all five technical areas. However, each technical area proposed must be submitted as a separate proposal. Proposers may receive awards for multiple technical areas. There are no conflicts between technical areas.

[2] https://www.acquisition.gov/FAR/.

IV. APPLICATION

A. Announcement

This announcement, the DD form 254 (Contract Security Classification Specification) and the Plan X Security Classification Guide (provided under separate cover) contains all information required to respond to this solicitation and constitutes the total BAA. No additional forms, kits, or other materials are needed. No request for proposal (RFP) or additional solicitation regarding this opportunity will be issued, nor is additional information available except as provided at the FedBizOpps website (http://www.fbo.gov) or referenced in this document.

Please note that a proposer MUST request and receive the Plan X Program SCG in order to effectively propose a classified submission to this BAA.

To obtain a copy of the Plan X Program SCG, proposers must send a request to the BAA mailbox, PlanX@darpa.mil, and include the following information:

Company name
Classified mailing address
CAGE Code
Facility Security Officer (FSO) name and phone number
Technical POC name and phone number

Note: DARPA will verify the facility clearance via the Industrial Security Facility Database (ISFD), including the ability to safeguard information and the clearance of the recipient before mailing the classified material. If the required clearances are not available, no classified material will be sent.

B. Proposals

Proposals consist of Volume 1: Technical and Management Proposal (including mandatory Appendix A and Appendix B) and Volume 2: Cost Proposal.

All pages shall be formatted for printing on 8-1/2 by 11-inch paper with a font size not smaller than 12 point. Font sizes of 8 or 10 point may be used for figures, tables, and charts.

Document files must be in .pdf, .odx, .doc, .docx, .xls, or .xlsx formats.

Submissions must be written in English.

Proposals not meeting the format prescribed herein may not be reviewed.

1. Volume 1: Technical and Management Proposal

The maximum count for Volume 1 is 40 pages, including all figures, tables and charts but not including the cover sheet, table of contents or appendices. A submission letter is optional and is not included in the page count. Appendix A does not count against the page limit and is mandatory. Appendix B does not count against the page limit and is mandatory. Additional information not explicitly called for here must not be submitted with the proposal, but may be included as links in the bibliography in Appendix B. Such materials will be considered for the reviewers' convenience only and not evaluated as part of the proposal. Resumes for each person on your team, including consultants and subcontractors, are mandatory.

Volume 1 must include the following components:

a. **Cover Sheet:** Include the following information.
   - Label: "Proposal: Volume 1"
   - BAA number (DARPA-BAA-13-02)
   - Proposal title
   - Lead organization (prime contractor) name
   - Type of business, selected from among the following categories: Large Business, Small Disadvantaged Business, Other Small Business, HBCU, MI, Other Educational, or Other Nonprofit
   - Technical point of contact including name, mailing address, telephone, and email
   - Administrative point of contact including name, mailing address, telephone, and email
   - Award instrument requested: procurement contract (specify type), grant, cooperative agreement or other transaction agreement.[3]
   - Place(s) and period(s) of performance
   - Other team member information (for each, include type of business and Technical point of contact name, mailing address, telephone, and email)
   - Proposal validity period (minimum 120 days)
   - DUNS number (http://fedgov.dnb.com/webform/index.jsp)
   - Taxpayer identification number (http://www.irs.gov/businesses/small/international/article/0,,id=96696,00.html)
   - CAGE code (http://www.dlis.dla.mil/CAGESearch/cage_faq.asp)
   - Contractor's reference number (if any)

b. **Table of Contents**

c. **Executive Summary:** Provide a synopsis of the proposed project, including answers to the following questions.

   - What are you trying to do?
   - How is it done today and what are the limitations?
   - Who will care and what will the impact be if you are successful?
   - How much will it cost, and how long will it take?

[3] Information on award instruments can be found at http://www.darpa.mil/Opportunities/Contract_Management/Contract_Management.aspx.

The summary should include a description of the key technical challenges, a concise review of the technologies proposed to overcome these challenges and achieve the project’s goal, and a clear statement of the novelty and uniqueness of the proposed idea.

d. **Goals and Impact:** Describe clearly what the team is trying to achieve and the difference it will make (qualitatively and quantitatively) if successful. Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the uniqueness and benefits of this project in the context of the state of the art, alternative approaches, and other projects from the past and present. Describe how the proposed project is revolutionary and how it significantly rises above the current state of the art.

Describe the deliverables associated with the proposed project and any plans to commercialize the technology, transition it to a customer, or further the work. Discuss the mitigation of any issues related to sustainment of the technology over its entire lifecycle, assuming the technology transition plan is successful.

e. **Technical Plan:** Outline and address technical challenges inherent in the approach and possible solutions for overcoming potential problems. Demonstrate a deep understanding of the technical challenges and present a credible (even if risky) plan to achieve the project’s goal. Discuss mitigation of technical risk. Provide appropriate measurable milestones (quantitative if possible) at intermediate stages of the project to demonstrate progress, and a plan for achieving the milestones.

f. **Management Plan:** Provide a summary of expertise of the team, including any subcontractors and key personnel who will be doing the work. Identify a principal investigator for the project. Provide a clear description of the team’s organization including an organization chart that includes, as applicable, the relationship of team members; unique capabilities of team members; task responsibilities of team members; teaming strategy among the team members; and key personnel with the amount of effort to be expended by each person during the project. Provide a detailed plan for coordination including explicit guidelines for interaction among collaborators/subcontractors of the proposed project. Include risk management approaches. Describe any formal teaming agreements that are required to execute this project. It is recommended that System Architecture (TA1) proposers include an Information Assurance team member certified in accordance with Department of Defense 8570.01-M, “Information Assurance Workforce Improvement Program.”

g. **Capabilities:** Describe organizational experience in this area, existing intellectual property, specialized facilities, and any Government-furnished materials or data. Discuss any work in closely related research areas and previous accomplishments.

h. **Statement of Work (SOW):** The SOW should provide a detailed task breakdown, citing specific tasks and their connection to the interim milestones and project metrics, as applicable. Each year of the project should be separately defined. The

SOW must not include proprietary information.

For each defined task/subtask, provide:

- A general description of the objective.
- A detailed description of the approach to be taken to accomplish each defined task/subtask.
- Identification of the primary organization responsible for task execution (prime contractor, subcontractor, team member, by name).
- A measurable milestone, i.e., a deliverable, demonstration, or other event that marks task completion.
- A definition of all deliverables (e.g., data, reports, and software) to be provided to the Government in support of the proposed research tasks/subtasks.
- A clear identification of any tasks/subtasks (by the prime or subcontractor) that will be accomplished on campus at a university.

i. Schedule and Milestones: Provide a detailed schedule showing tasks (task name, duration, work breakdown structure element as applicable, performing organization), milestones, and the interrelationships among tasks. The task structure must be consistent with that in the SOW. Measurable milestones should be clearly articulated and defined in time relative to the start of project.

j. Cost Summary: Provide the cost summary as described in Section IV.B.2.b.

k. Appendix A: This section is mandatory and must include all the following components. If a particular subsection is not applicable, state “NONE.”

(i) Team Member Identification: Provide a list of all team members (prime and subcontractors). Identify specifically whether any are a non-US organization or individual, FFRDC and/or Government entity. The following format should be used for this list:

Prime	**Organization**	**Non-US?**	**FFRDC or Government?**
Subcontractor	**Organization**	**Non-US?**	**FFRDC or Government?**
Consultant	**Organization**	**Non-US?**	**FFRDC or Government?**

(ii) Government or FFRDC Team Member Authority to Propose to this BAA: If none of the team member organizations (prime or subcontractor) are a Government entity or FFRDC, state “NONE.”

If any of the team member organizations are a Government entity or FFRDC, provide documentation (per Section III.A.2) citing the specific authority that establishes the applicable team member as eligible to propose to Government solicitations to include: 1) statutory authority; 2) contractual authority; 3) supporting regulatory guidance; and 4) evidence of agency approval for applicable team member participation.

(iii) Government or FFRDC Team Member Statement of Unique Capability: If none of the team member organizations (prime or subcontractor) are a Government entity or FFRDC, state "NONE."

If any of the team member organizations are a Government entity or FFRDC, provide a statement that demonstrates the work being provided by the Government entity or FFRDC team member is not otherwise available from the private sector.

(iv) Organizational Conflict of Interest Affirmations and Disclosure: If all of the proposed team members are not currently providing SETA support as described in Section III.B, state "NONE."

If any of the proposed team members (individual or organization) is currently providing SETA support, provide the following information:

Prime Contract Number	DARPA Office supported	A description of the action the proposer has taken or proposes to take to avoid, neutralize, or mitigate the conflict

(v) Intellectual Property: If no intellectual property restrictions are intended, state "NONE." The Government will assume unlimited rights to all intellectual property not explicitly identified as restricted in the proposal.

For all technical data or computer software that will be furnished to the Government with other than unlimited rights, provide (per Section VI.B.2) a list describing all proprietary claims to results, prototypes, deliverables or systems supporting and/or necessary for the use of the research, results, prototypes and/or deliverables. Provide documentation proving ownership or possession of appropriate licensing rights to all patented inventions (or inventions for which a patent application has been filed) to be used for the proposed project. The following format should be used for this list:

NONCOMMERCIAL				
Technical Data and/or Computer Software To be Furnished With Restrictions	**Summary of Intended Use in the Conduct of the Research**	**Basis for Assertion**	**Asserted Rights Category**	**Name of Person Asserting Restrictions**
(LIST)	(Narrative)	(LIST)	(LIST)	(LIST)

COMMERCIAL				
Technical Data and/or Computer Software To be Furnished With Restrictions	**Summary of Intended Use in the Conduct of the Research**	**Basis for Assertion**	**Asserted Rights Category**	**Name of Person Asserting Restrictions**
(LIST)	(Narrative)	(LIST)	(LIST)	(LIST)

(vi) Human Use: If human use is not a factor in a proposal, state "NONE."

If the proposed research will involve human subjects in the first year or phase of the project, provide evidence of or a plan for review by an institutional review board (IRB). For further information on this subject, see Section VI.B.3.

(vii) Animal Use: If animal use is not a factor in a proposal, state "NONE."

If the proposed research will involve animal use, provide a brief description of the plan for Institutional Animal Care and Use Committee (IACUC) review and approval. For further information on this subject, see Section VI.B.4.

(viii) Representations Regarding Unpaid Delinquent Tax Liability or a Felony Conviction under Any Federal Law: Per Section VI.B.11, complete the following statements.

(1) The proposer represents that it is [ ] is not [ ] a corporation that has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability.

(2) The proposer represents that it is [ ] is not [ ] a corporation that was convicted of a felony criminal violated under Federal law within the preceding 24 months.

(ix) Cost Accounting Standards Notices and Certification: Per Section VI.B.12, any proposer who submits a proposal which, if accepted, will result in a cost accounting standards (CAS) compliant contract, must include a Disclosure Statement as required by 48 CFR 9903.202. The disclosure forms may be found at http://www.whitehouse.gov/omb/procurement_casb.

If this section is not applicable, state "NONE."

(x) Subcontractor Plan: Pursuant to Section 8(d) of the Small Business Act (15 U.S.C. § 637(d)), it is Government policy to enable small business and small disadvantaged business concerns to be considered fairly as subcontractors to organizations performing work as prime contractors or subcontractors under Government contracts, and to ensure that prime contractors and subcontractors carry out this policy. If applicable, prepare a subcontractor plan in accordance with FAR 19.702(a) (1) and (2). The plan format is outlined in FAR 19.704.

If this section is not applicable, state “NONE.”

l. **Appendix B:** Include resumes from each person on your team, including security, consultants and subcontractors, highlighting particular experience in the proposed research area. If desired, include a brief bibliography with links to relevant papers, reports, or resumes. Do not include technical papers. The linked materials will not be evaluated as part of the proposal review.

2. Volume 2 - Cost Proposal

This volume is mandatory and must include all the listed components. No page limit is specified for this volume.

a. **Cover Sheet:** Include the same information as the cover sheet for Volume 1 with the label “Proposal: Volume 2.”

b. **Cost Summary:** Provide a single-page summary with cost totals for labor, materials, other direct charges (ODCs), indirect costs (overhead, fringe, general and administrative (G&A)), and the proposed fee (if any) for the project by year. Include costs for each task in each year of the project by prime and major subcontractors, total cost and proposed cost share, if applicable. Include any requests for Government-furnished equipment or information with cost estimates (if applicable) and delivery dates.

c. **Detailed Cost Information:** Provide detailed cost information for direct labor (including labor categories), materials, ODCs and indirect costs by month for each task of the project. Information provided for subcontractors must be at the same level of detail as that provided for prime contractors. Both labor rates and hours should be detailed. A separate breakdown should be done for any proposed option(s).

Summarize task-level cost information to give total expenditures on labor, materials, indirect costs and ODCs by month for prime and subcontractors. Identify cost sharing (if any). Itemize purchases of information technology (as defined in FAR 2.101). Provide totals for all cost categories.

The cost proposal should include a spreadsheet file (.xls or equivalent format) that provides formula traceability among all components of the cost proposal. Costs must be traceable between prime and subcontractor as well as between the cost proposal and the statement of work. The spreadsheet file should be included as a separate component of the full proposal package.

For proposed information technology and equipment purchases that are equal to or greater than $50,000 for a single item, a letter should be included justifying the purchase.

Proposers without a Defense Contract Audit Agency-approved cost accounting system who are requesting a cost-type contract must include a completed form SF 1408 in the proposal in order for the submission to be deemed conforming to this solicitation. The SF 1408 form can be found at https://www.acquisition.gov/far/html/FormsStandard41.html.

Supporting cost and pricing information shall include a description of the method used to estimate costs and supporting documentation. “Certified cost or pricing data” as defined in FAR 15.4 shall be required if the proposer is seeking a procurement contract award of $700,000 or greater unless the proposer requests an exception from the requirement to submit this information. Certified cost or pricing data is not required if the proposer proposes an award instrument other than a procurement contract (e.g., a grant, cooperative agreement, or other transactions).

Pre-award costs are not reimbursable for awards under this BAA.

See Section III.C for information on cost sharing/matching.

A cost proposal checklist is provided in Section VIII.C. Nonconforming proposals may be rejected without review.

d. **Subcontractors:** The proposer is responsible for the compilation and submission of all subcontractor cost proposals. Proposal submissions will not be considered complete until the Government has received all subcontractor cost proposals.

Proprietary subcontractor cost proposals may be included as part of Volume 2 or submitted separately to PlanX@darpa.mil (not uploaded to the submission site). Email messages should include “Subcontractor Cost Proposal” in the subject line and identify the principal investigator and prime proposer organization in the message.

Subcontractor cost proposals should include interdivisional work transfer agreements or similar arrangements.

e. **Other Transactions:** If the proposer requests award of an 845 Other Transactions Agreement (OTA) as a nontraditional defense contractor, as defined in the OSD guide “Other Transactions (OT) Guide For Prototype Projects” dated January 2001 (as amended) (http://www.acq.osd.mil/dpap/Docs/otguide.doc), information must be included in the cost proposal to support the claim. If the proposer requests award of an 845 OT agreement without the required one-third (1/3) cost share, information must be included in the cost proposal supporting the claim that there is at least one nontraditional Defense contractor participating to a significant extent in the proposed prototype project.

Proposers requesting an 845 OT for Prototypes agreement must include a detailed list of milestones including: milestone description, completion criteria, due date, and payment/funding schedule (to include, if cost share is proposed, contractor and Government share amounts). Milestones should relate directly to accomplishment of technical metrics as defined in the BAA and/or the proposal. Agreement type, fixed price or expenditure based, will be subject to negotiation with DARPA; however, the use of fixed price milestones with a payment/funding schedule is preferred. Proprietary information must not be included as part of the milestones.

For information on 845 OTs, refer to http://www.darpa.mil/Opportunities/Contract_Management/Other_Transactions_and_Technology_Investment_Agreements.aspx.

C. Proprietary and Classified Information

1. Proprietary Information

DARPA policy is to treat all submissions as source selection information (see FAR 2.101 and 3.104) and to disclose the contents only for the purpose of evaluation.

Proposers are responsible for identifying proprietary information to DARPA. Submissions containing proprietary information must have the cover page and each page containing such information clearly marked. Proprietary information must not be included in the proposed schedule, milestones, or SOW.

Restrictive notices notwithstanding, during the evaluation process, submissions may be handled by support contractors for administrative purposes and/or to assist with technical evaluation. All DARPA support contractors performing this role are expressly prohibited from performing DARPA-sponsored technical research and are bound by appropriate nondisclosure agreements.

2. Classified Information

DARPA anticipates that Volume 1 (Technical and Management Proposal) submissions received under this BAA may be unclassified, collateral SECRET in accordance with the Plan X Program SCG, SECRET//NOFORN, and/or SECRET//REL TO depending upon if derivative classification is applied from other appropriately marked references. **Proposal submissions at higher classification levels above collateral SECRET will not be accepted**. See Section IV.D.2 for further instructions regarding classified submissions. Volume 2 (Cost Proposal) must be unclassified. Guidance regarding marking, packing and delivery of classified proposals is provided in the DD Form 254, “Contact Security Classification Specification.”

Classified submissions shall be appropriately and conspicuously marked with the proposed classification level and declassification date. Classified submissions must indicate the classification level of not only the submitted materials, but also the anticipated classification level of the award document. Applicable classification guide(s) must be included to ensure the submission is protected at the appropriate classification level.

If a proposer believes a submission contains classified information (as defined by Executive Order 13526), but requires DARPA to make a final classification determination, the information must be marked and protected as though classified at the appropriate classification level (as defined by Executive Order 13526).

Submissions requesting DARPA to make a final classification determination shall be marked as follows:

> "CLASSIFICATION DETERMINATION PENDING. Protect as though classified ____________________ *[insert the recommended classification level, e.g., Confidential, Secret, or Top Secret]."*

Proposers submitting classified proposals or requiring access to classified information during the lifecycle of the project shall ensure all industrial, personnel, and information system processing security requirements (e.g., facility clearance (FCL), personnel security clearance (PCL), certification and accreditation (C&A)) are in place and at the appropriate level, and any foreign ownership control and influence (FOCI) issues are mitigated prior to submission or access. Proposers must have existing, approved capabilities (personnel and facilities) prior to award to perform research and development at the classification level proposed. Additional information on these subjects is at http://www.dss.mil.

After an incoming proposal is reviewed and a determination has been made that the award instrument may result in access to classified information, a DD Form 254, "DoD Contract Security Classification Specification," will be issued and attached as part of the award. A DD Form 254 will not be provided at the time of submission. The DD Form 254 template is available at http://www.dtic.mil/dtic/pdf/formsNguides/dd0254.pdf.

Classified submissions will not be returned. The original of each classified submission received will be retained at DARPA, and all other copies destroyed. A destruction certificate will be provided if a formal request is received by DARPA within 5 days of notification of non-selection.

D. Submission Instructions

1. Due Dates

The proposal package--full proposal (Volume 1 and 2) and, as applicable, proprietary subcontractor cost proposals--must be submitted per the instructions outlined in this document and received by DARPA by the proposal closing date of January 25, 2013, 1200 noon (ET). Submissions received after this time will not be reviewed.

Proposers are warned that submission deadlines as outlined herein are strictly enforced.

DARPA will acknowledge receipt of complete submissions via email and assign control numbers that should be used in all further correspondence regarding proposals. Note: these acknowledgements will not be sent until after the proposal due date, as applicable.

Failure to comply with the submission procedures may result in the submission not being evaluated.

2. Unclassified Submission

All unclassified proposals shall be submitted to DARPA/I2O, 675 North Randolph Street, Arlington, VA 22203-2114 (Attn: BAA Coordinator). Unclassified proposals must not be submitted electronically by any means (e.g., unclassified fax, email, etc.). Any so sent WILL be disregarded.

Proposers must submit an original and one (1) hard copy of the unclassified proposal (Technical and Cost volumes) and two (2) electronic copies of the unclassified proposal, each on an individual CD-ROM.

3. Classified Submission

Classified submissions must be appropriately marked and must not be submitted electronically by any means, (unclassified fax, email, etc.). Use classification and marking guidance provided by the DoD Information Security Manual (DoDM 5200.1, Volumes 1-4) and the National Industrial Security Program Operating Manual (DoD 5220.22-M). When marking and transmitting information previously classified by another OCA, also use the applicable security classification guides.

Proposers must submit an original and one (1) hard copy of the technical proposal and two (2) electronic copies of the technical proposal, each on an individual CD-ROM. Proposers must also provide an original and one (1) hard copy of the unclassified cost proposal and two (2) electronic copies of the unclassified cost proposal, each on an individual CD-ROM. The electronic versions are preferred in Portable Document Format (.pdf ISO 32000-1) and will be on a CD-ROM. However, the CD-ROMs must also include the original of the documents (e.g., .doc or .xls formats) used to create the .pdf files.

Proposals must not be submitted electronically by any means. Any so sent WILL be disregarded. Unclassified email at PlanX@darpa.mil can be used to communicate with DARPA regarding this solicitation, but DO NOT include any classified information.

Classified materials must be submitted in accordance with the following guidelines:

a. **Confidential and Secret Collateral Information:** Classified information at the Confidential or Secret level may be submitted by one of the following methods:

   - Hand carried by an appropriately cleared and authorized courier to DARPA. Prior to traveling, the courier shall contact the DARPA Classified Document Registry (CDR) at 703-526-4052 to coordinate arrival and delivery.

     or

   - Mailed by U.S. Postal Service Registered Mail or Express Mail. All classified information will be enclosed in opaque inner and outer covers and double wrapped.

The inner envelope shall be sealed and plainly marked with the assigned classification and addresses of both sender and addressee. The inner envelope shall be addressed to:

Defense Advanced Research Projects Agency
ATTN: I2O BAA Coordinator
Reference: DARPA-BAA-13-02
675 North Randolph Street
Arlington, VA 22203-2114

The outer envelope shall be sealed without identification as to the classification of its contents and addressed to:

Defense Advanced Research Projects Agency
Security & Intelligence Directorate, Attn: CDR
675 North Randolph Street
Arlington, VA 22203-2114

DARPA does not anticipate any submissions above collateral SECRET; however if higher-leveled information is needed in your proposal, please contact us at PlanX@darpa.mil for instructions.

E. Intergovernmental Review

Not applicable.

F. Funding Restrictions

Not applicable.

V. EVALUATION

A. Evaluation Criteria

Evaluation of proposals will be accomplished through a scientific/technical review of each proposal using the following criteria listed in descending order of importance: Overall Scientific and Technical Merit; Potential Contribution and Relevance to the DARPA Mission; and Cost Realism.

- **Overall Scientific and Technical Merit:** The proposed technical approach is feasible, achievable, complete and supported by a proposed technical team that has the expertise and experience to accomplish the proposed tasks. The task descriptions and associated technical elements are complete and in a logical sequence, with all proposed deliverables clearly defined such that a viable attempt to achieve project goals is likely as a result of award. The proposal identifies major technical risks and clearly defines feasible mitigation efforts. The proposal addresses the commercial product experience and technical expertise of the team to include consultants and subcontractors.

- **Potential Contribution and Relevance to the DARPA Mission:** The potential contributions of the proposed project are relevant to the national technology base. Specifically, DARPA's mission is to maintain the technological superiority of the U.S. military and prevent technological surprise from harming our national security by sponsoring revolutionary, high-payoff research that bridges the gap between fundamental discoveries and their application.

- **Cost Realism:** The proposed costs are based on realistic assumptions, reflect a sufficient understanding of the technical goals and objectives of the BAA, and are consistent with the proposer's technical/management approach (to include the proposed SOW). The costs for the prime and subcontractors are substantiated by the details provided in the proposal (e.g., the type and number of labor hours proposed per task, the types and quantity of materials, equipment and fabrication costs, travel and any other applicable costs).

B. Review and Selection Process

DARPA policy is to ensure impartial, equitable, comprehensive proposal evaluations and to select sources whose offers meet the DARPA technical, policy, and programmatic goals.

In order to provide the desired evaluation, qualified Government personnel will conduct reviews and (if necessary) convene panels of experts in the appropriate areas. Subject to the restrictions set forth in FAR 37.203(d), input on technical aspects of the proposals may be solicited by DARPA from non-Government consultants/experts who are strictly bound by appropriate nondisclosure requirements.

The review process identifies proposals that meet the established criteria and are, therefore, selectable for funding awards by the Government. Selections under this BAA will be made to proposers on the basis of the evaluation criteria listed in Section V.A. Proposals that are determined to be selectable will not necessarily receive awards. Selections may be made at any time during the period of solicitation.

Failure to comply with the submission procedures may result in the submission not being evaluated. Classified proposals WILL NOT be returned. The original of each classified proposal received will be retained at DARPA, and all other copies destroyed.

VI. AWARD ADMINISTRATION

A. Selection Notices

After proposal evaluation is complete, proposers will be notified whether their proposals are selectable as determined by the review process. Notification will be sent by email to the technical and administrative POCs identified on the proposal cover sheet. If a proposal has been selected, the Government will initiate award negotiations following the notification.

B. Administrative and National Policy Requirements

1. Meeting and Travel Requirements

Performers should anticipate weekly visits at the CRS by the DARPA Program Manager with only occasional site visits at the performer’s home site, at the DARPA Program Manager’s discretion. Off-site performers are expected to travel to the CRS in Arlington, VA with the whole team for four one-week design checkpoints per phase.

2. Intellectual Property

It is desired that all noncommercial software (including source code), software documentation, hardware designs and documentation, and technical data generated under the program be provided as a deliverable to the Government, with a minimum of Government Purpose Rights (GPR). Therefore, to the greatest extent feasible, proposers should not include background proprietary software and technical data as the basis of their proposed approach.

Proposers expecting to use, but not to deliver, commercial open source tools or other materials in implementing their approach may be required to indemnify the Government against legal liability arising from such use.

All references to "Unlimited Rights" or "Government Purpose Rights" are intended to refer to the definitions of those terms as set forth in the Defense Federal Acquisition Regulation Supplement (DFARS) Part 227.

a. Procurement Contracts

- **Noncommercial Items (Technical Data and Computer Software):** Proposers responding to this BAA requesting a procurement contract shall list all noncommercial technical data and computer software that it plans to generate, develop, and/or deliver under any proposed award instrument in which the Government will acquire less than unlimited rights and to assert specific restrictions on those deliverables. A sample list for complying with this request is provided in Section IV.B.1.k.(v). In the event proposers do not submit the list, the Government will assume that it has “unlimited rights” to all noncommercial technical data and computer software generated, developed, and/or delivered under any award instrument, unless it is substantiated that development of the noncommercial technical data and computer software occurred with mixed funding. If mixed funding is anticipated in the development of noncommercial technical data and computer software generated, developed, and/or delivered under any award instrument, proposers should identify the data and software in question as subject to GPR. In accordance with DFARS 252.227-7013, "Rights in Technical Data - Noncommercial Items," and DFARS 252.227-7014, "Rights in Noncommercial Computer Software and Noncommercial Computer Software Documentation," the Government will automatically assume that any such GPR restriction is limited to a period of 5 years, at which time the Government will acquire unlimited rights unless the parties agree otherwise. The Government may use the list during the evaluation process to evaluate the impact of any identified restrictions and may request additional information from the proposer, as may be necessary, to evaluate the proposer's assertions. Failure to provide full information may result in a determination that the proposal is not compliant with the BAA. If no restrictions are intended, the proposer should state "NONE."

- **Commercial Items (Technical Data and Computer Software):** Proposers responding to this BAA requesting a procurement contract shall list all commercial technical data and commercial computer software that may be included in any noncommercial deliverables contemplated under the research project, and assert any applicable restrictions on the Government's use of such commercial technical data and/or computer software. A sample list for complying with this request is provided in Section IV.B.1.k.(v). In the event proposers do not submit the list, the Government will assume there are no restrictions on the Government's use of such commercial items. The Government may use the list during the evaluation process to evaluate the impact of any identified restrictions and may request additional information from the proposer to evaluate the proposer's assertions. Failure to provide full information may result in a determination that the proposal is not compliant with the BAA. If no restrictions are intended, the proposer should state "NONE."

b. Patents: Proposers must include documentation proving ownership or possession of appropriate licensing rights to all patented inventions to be used for the proposed project. If a patent application has been filed for an invention, but it includes proprietary information and is not publicly available, a proposer must provide documentation that includes: the patent number, inventor name(s), assignee names (if any), filing date, filing date of any related provisional application, and summary of the patent title, with either: (1) a representation of invention ownership, or (2) proof of possession of appropriate licensing rights in the invention (i.e., an agreement from the owner of the patent granting license to the proposer).

c. Intellectual Property Representations: Proposers should provide a good faith representation of either ownership or possession of appropriate licensing rights to all other intellectual property to be used for the proposed project. Proposers shall provide a short summary for each item asserted with less than unlimited rights that describes the nature of the restriction and the intended use of the intellectual property in the conduct of the proposed research.

3. Human Use

All research involving human subjects, to include use of human biological specimens and human data, selected for funding must comply with Federal regulations 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"[4] and DoD Directive 3216.02, "Protection of Human Subjects and Adherence to Ethical Standards in DoD-Supported Research."[5]

Institutions awarded funding for research involving human subjects must provide documentation of a current Assurance of Compliance with Federal regulations for human subject protection, for example a Department of Health and Human Services, Office of Human Research Protection Federal Wide Assurance.[6] All institutions engaged in human subject research, to include subcontractors, must have a valid assurance. In addition, personnel involved in human subject research must document the completion of appropriate training for the protection of human subjects.

For all research that will involve human subjects in the first year or phase of the project, the institution must submit evidence of a plan for review by an institutional review board (IRB) as part of the proposal. The IRB conducting the review must be the IRB identified on the institution's Assurance of Compliance. 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. The designated IRB should be consulted for guidance on writing the protocol. The informed consent document must comply with 32 CFR 219.116. A valid Assurance of Compliance and evidence of appropriate training by all investigators should accompany the protocol for review by the IRB.

In addition to a local IRB approval, a headquarters-level human subjects regulatory review and approval is required for all research conducted or supported by DoD. The Army, Navy, or Air Force office responsible for managing the award can provide guidance and information about their component's headquarters-level review process. Confirmation of a current Assurance of Compliance and appropriate human subjects protection training is required before headquarters-level approval can be issued.

The time required to complete the IRB review/approval process will 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 IRB approval process can last between 1 to 3

[4] http://www.access.gpo.gov/nara/cfr/waisidx_07/32cfr219_07.html
[5] http://www.dtic.mil/whs/directives/corres/pdf/321602p.pdf
[6] http://www.hhs.gov/ohrp

months, followed by a DoD review that could last 3 to 6 months. No DoD/DARPA funding may be used toward human subject research until all approvals are granted.

4. Animal Use

Award recipients performing research, experimentation, or testing involving the use of animals shall comply with the rules on animal acquisition, transport, care, handling, and use as outlined in:

- 9 CFR Parts 1-4, Department of Agriculture regulation that implements the Animal Welfare Act of 1966, as amended (7 U.S.C. §§ 2131-2159);
- National Institutes of Health Publication No. 86-23, "Guide for the Care and Use of Laboratory Animals"; and
- DoD Directive 3216.01, "Use of Animals in DoD Programs."

For projects anticipating animal use, proposals should briefly describe plans for Institutional Animal Care and Use Committee (IACUC) review and approval. Animal studies in the program will be expected to comply with the "Public Health Service Policy on Humane Care and Use of Laboratory Animals."[7]

All award recipients must receive approval by a DoD-certified veterinarian, in addition to IACUC approval. No animal studies may be conducted using DoD/DARPA funding until the U.S. Army Medical Research and Materiel Command Animal Care and Use Review Office (ACURO) or other appropriate DoD veterinary office(s) grant approval. As a part of this secondary review process, the recipient will be required to complete and submit an ACURO Animal Use Appendix.[8]

5. Publication Approval and Fundamental Research

It is DoD policy that the publication of products of fundamental research will remain unrestricted to the maximum extent possible. Per DoD Directive 5230.27, contracted fundamental research "includes [research performed under] grants and contracts that are (a) funded by budget category 6.1 (Basic Research), whether performed by universities or industry, or (b) funded by budget category 6.2 (Applied Research) and performed on campus at a university. The research shall not be considered fundamental in those rare and exceptional circumstances where the applied research effort presents a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense, and where agreement on restrictions have been recorded in the contract or grant." Such research is referred to by DARPA as "restricted research."

Pursuant to DoD policy, research performed under DoD awards that is either: (a) funded by budget category 6.2 (Applied Research) and not performed on campus at a university; or (b) funded by budget category 6.3 (Advanced Research) does not meet the definition of fundamental research. Such research is referred to by DARPA as "non-fundamental research."

For certain projects, even if the effort being performed by the prime contractor is restricted

[7] http://grants.nih.gov/grants/olaw/olaw.htm

[8] https://mrmc.amedd.army.mil/index.cfm?pageid=Research_Protections.acuroAnimalAppendix

research, a subcontractor may be performing contracted fundamental research. In these cases, it is the prime contractor's responsibility to explain in the proposal why the subcontractor's effort is contracted fundamental research.

It is anticipated that awards for non-fundamental and restricted research may be made as a result of this BAA. Appropriate clauses will be included in resultant awards for restricted and non-fundamental research to prescribe publication requirements and other restrictions, as appropriate. DARPA does not anticipate applying publication restrictions of any kind to awards for fundamental research that may result from this BAA.

Proposers are advised that, if grants or cooperative agreements are proposed as the award instrument, DARPA may elect to award other award instruments due to the need to apply publication or other restrictions. DARPA will make this election if it determines that research resulting from the proposed project will present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Such a determination will result in the project being considered restricted research and any resultant award will include a requirement for DARPA permission before publishing any information or results on the project.

The following statements or similar provisions will be incorporated into any resultant procurement contract or other transactions for restricted or non-fundamental research:

> There shall be no dissemination or publication, except within and between the contractor and any subcontractors, of information developed under this contract or contained in the reports to be furnished pursuant to this contract without prior written approval of the DARPA Public Release Center (PRC). All technical reports will be given proper review by appropriate authority to determine which distribution statement is to be applied prior to the initial distribution of these reports by the contractor. With regard to subcontractor proposals for contracted fundamental research, papers resulting from unclassified contracted fundamental research are exempt from prepublication controls and this review requirement, pursuant to DoD Instruction 5230.27 'Presentation of DoD-Related Scientific and Technical Papers at Meetings.'
>
> When submitting material for written approval for open publication, the contractor/awardee must submit a request for public release to the DARPA PRC and include the following information: 1) Document Information: title, author, short plain-language description of technology discussed in the material (approximately 30 words), number of pages (or minutes of video) and document type (briefing, report, abstract, article, or paper); 2) Event Information: type (conference, principal investigator meeting, article or paper), date, and desired date for DARPA's approval; 3) DARPA Sponsor: DARPA program manager, DARPA office, and contract number; and 4) Contractor/Awardee's information: POC name, email and telephone. Four weeks should be allowed for processing; due dates under four weeks may require justification. Unusual electronic file formats may require additional processing time. Requests can be sent either by email to prc@darpa.mil or mail to 675 North Randolph Street, Arlington VA 22203-2114, 571-218-4235.

More information regarding DARPA's public release process may be found at http://www.darpa.mil/NewsEvents/Public_Release_Center/Public_Release_Center.aspx.

6. Export Control

Per DFARS 204.7304, all procurement contracts and other transactions, as deemed appropriate, resultant from this solicitation will include the DFARS Export Control clause (252.204-7008).

7. Electronic and Information Technology

All electronic and information technology acquired through this solicitation must satisfy the accessibility requirements of Section 508 of the Rehabilitation Act (29 U.S.C. § 794d) and FAR 39.2. Each project involving the creation or inclusion of electronic and information technology must ensure that: (1) 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, and (2) members of the public with disabilities seeking information or services from DARPA 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.

8. Employment Eligibility Verification

Per FAR 22.1802, recipients of FAR-based procurement contracts must enroll as Federal contractors in E-verify[9] and use the system to verify employment eligibility of all employees assigned to the award. All resultant contracts from this solicitation will include the clause at FAR 52.222-54, "Employment Eligibility Verification." This clause will not be included in grants, cooperative agreements, or other transactions.

9. Reporting Executive Compensation and First-Tier Subcontract Awards

Per FAR 4.1403, FAR-based procurement contracts valued at $25,000 or more will include the clause at FAR 52.204-10, "Reporting Executive Compensation and First-Tier Subcontract Awards." A similar award term will be used in grants, cooperative agreements, and other transactions. This clause is not required in classified contracts.

10. Updates of Information Regarding Responsibility Matters

Per FAR 9.104-7(c), 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.

11. Representation by Corporations Regarding Unpaid Delinquent Tax Liability or a Felony Conviction under Any Federal Law

[9] http://www.uscis.gov/e-verify

In accordance with the Consolidated Appropriations Act, 2012 (Pub. L. 112-74), none of the funds made available by that Act may be used to enter into a contract with any corporation that: (1) has any unpaid Federal tax liability that has been assessed, for which all judicial and administrative remedies have been exhausted or have lapsed, and that is not being paid in a timely manner pursuant to an agreement with the authority responsible for collecting the tax liability, unless the agency has considered suspension or debarment of the corporation and made a determination that this further action is not necessary to protect the interests of the Government; or (2) was convicted of a felony criminal violation under any Federal or State law within the preceding 24 months, where the awarding agency is aware of the conviction, unless the agency has considered suspension or debarment of the corporation and made a determination that this action is not necessary to protect the interests of the Government. Each proposer must complete and return the representations outlined in Section IV.C.1.k.(vii) with their proposal submission.

12. Cost Accounting Standards Notices and Certification

Per FAR 52.230-2, amended by Deviation 2012-00003 (JAN 2012), any procurement contract in excess of $700,000 resulting from this solicitation will be subject to the requirements of the Cost Accounting Standards Board (48 CFR 99), except those contracts which are exempt as specified in 48 CFR 9903.201-1. Any proposer who submits a proposal which, if accepted, will result in a cost accounting standards (CAS) compliant contract, must include a Disclosure Statement as required by 48 CFR 9903.202. The disclosure forms may be found at http://www.whitehouse.gov/omb/procurement_casb.

13. Providing Accelerated Payment to Small Business Subcontractors (DEVIATION)

The following clause, which implements the temporary policy provided by OMB Policy Memorandum M-12-16, Providing Prompt Payment to Small Business Subcontractors, dated July 11, 2012, will be included in all FAR-based awards:

(a) Upon receipt of accelerated payments from the Government, the contractor is required to make accelerated payments to small business subcontractors to the maximum extent practicable after receipt of a proper invoice and all proper documentation from the small business subcontractor.

(b) Include the substance of this clause, including this paragraph (b), in all subcontracts with small business concerns.

(c) The acceleration of payments under this clause does not provide any new rights under the Prompt Payment Act.

14. Controlled Unclassified Information (CUI) on Non-DoD Information Systems

CUI refers to unclassified information that does not meet the standards for National Security Classification but is pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government and under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. All non-DoD entities doing business with DARPA are expected to adhere to the following procedural safeguards, in addition to any other relevant Federal or DoD specific procedures, for submission of any proposals to DARPA and any potential business with DARPA:

- Do not process DARPA CUI on publicly available computers or post DARPA CUI to publicly available webpages or websites that have access limited only by domain or Internet protocol restriction.
- Ensure that all DARPA CUI is protected by a physical or electronic barrier when not under direct individual control of an authorized user and limit the transfer or DARPA CUI to subcontractors or teaming partners with a need to know and commitment to this level of protection.
- Ensure that DARPA CUI on mobile computing devices is identified and encrypted and all communications on mobile devices or through wireless connections are protected and encrypted.
- Overwrite media that has been used to process DARPA CUI before external release or disposal.

C. Reporting

The number and types of technical and financial reports required under the contracted effort will be specified in the award document, and will include, at a minimum, monthly financial status reports and a yearly status summary. The reports shall be prepared and submitted in accordance with the procedures contained in the award document. A final report that summarizes the project and tasks will be required at the conclusion of the performance period for the award.

D. Electronic Systems

1. System for Award Management (SAM) Registration and Universal Identifier Requirements

Unless the proposer is exempt from this requirement, as per FAR 4.1102 or 2 CFR 25.110, as applicable, all proposers must be registered in the SAM and have a valid Data Universal Numbering System (DUNS) number prior to submitting a proposal. All proposers must provide their DUNS number in each proposal they submit. All proposers must maintain an active SAM registration with current information at all times during which they have an active Federal award or proposal under consideration by DARPA. DARPA cannot make an award unless the proposer has provided a valid DUNS number and has an active SAM registration with current information. Information on SAM registration is available at http://www.sam.gov.

2. Representations and Certifications

In accordance with FAR 4.1201, prospective proposers shall complete electronic annual representations and certifications at http://www.sam.gov.

3. Wide Area Work Flow (WAWF)

Performers are required to submit invoices for payment directly at https://wawf.eb.mil. WAWF registration is required prior to any award under this BAA.

4. i-Edison

The award document for each proposal selected for funding will contain a requirement for patent reports and notifications to be submitted electronically through the i-Edison Federal patent reporting system at http://s-edison.info.nih.gov/iEdison.

5. Technical – Financial Information Management System (T-FIMS):

Financial and Technical status reports must be submitted electronically at https://www.tfims.darpa.mil.

VII. AGENCY CONTACTS

DARPA will use email for all unclassified technical and administrative correspondence regarding this BAA.

- Technical POC: Daniel Roelker, Program Manager, DARPA I2O

- Email: PlanX@darpa.mil

- Mailing address:
  - DARPA I2O
  - ATTN: DARPA-BAA-13-02
    675 North Randolph Street
    Arlington, VA 22203-2114

- Website: http://www.darpa.mil/Opportunities/Solicitations/I2O_Solicitations.aspx

VIII. OTHER INFORMATION

A. Frequently Asked Questions (FAQs)

Unclassified administrative, technical, and contractual questions should be sent via email to PlanX@darpa.mil. All requests must include the name, email address, and the phone number of a point of contact.

DARPA will attempt to answer questions in a timely manner; however, questions submitted within 7 days of initial closing may not be answered. If applicable, DARPA will post FAQs to http://www.darpa.mil/Opportunities/Solicitations/I2O_Solicitations.aspx.

B. Proposers' Day Workshop

The Proposers' Day Workshop was held October 15 and 16, 2012 in Arlington, VA.

Proposers may request a copy of the materials presented at the Plan X Proposers' Day Workshop per the guidance found in Special Notice DARPA-SN-13-02, which was posted to FBO website on October 23, 2012. Please note that such requests should be to PlanX@darpa.mil no later than 5:00 PM (ET) on November 30, 2012.

C. Submission Checklist

The following items apply prior to proposal submission:

✓	Item	BAA Section	Applicability	Comment
	Obtain DUNS number	IV.B.1.a	Required on proposal cover page	http://fedgov.dnb.com/webform/index.jsp The DUNS Number is the Federal Government's contractor identification code for all procurement-related activities.
	Enroll in the System for Award Management (SAM)	VI.D.1	Required of all proposers	www.sam.gov The SAM combines federal procurement systems and the Catalog of Federal Domestic Assistance into one new system. SAM currently includes the functionality from the following systems: * Central Contractor Registry (CCR) * Federal Agency Registration (Fedreg) * Online Representations and Certifications Application (ORCA) * Excluded Parties List System (EPLS)
	Obtain Taxpayer Identification Number (TIN)	IV.C.1.a	Required on proposal cover page	http://www.irs.gov/businesses/small/international/article/0,,id=96696,00.html A TIN is used by the Internal Revenue Service in the administration of tax laws.
	Obtain CAGE code	IV.C.1.a	Required on proposal cover page	http://www.dlis.dla.mil/CAGESearch/cage_faq.asp A CAGE Code identifies companies doing or wishing to do business with the Federal Government.

	Enroll in E-Verify	VI.B.8	Applies to FAR-based contracts, not to grants, cooperative agreements, or other transactions	http://www.uscis.gov/e-verify E-Verify is an Internet-based system that allows businesses to determine the eligibility of their employees to work in the United States.
	Ensure representations and certifications are up to date	VI.D.2	Required of all proposers	http://www.sam.gov Federal provisions require entities to represent/certify to a variety of statements ranging from environmental rules compliance to entity size *representation*.
	Ensure eligibility of all team members	III	Required of all proposers (primes and subcontractors)	Verify eligibility, as applicable, for FFRDCs, Government entities, organizational conflict of interest.

The following items apply as part of the submission package:

✓	**Item**	**BAA Section**	**Applicability**	**Comment**
	Volume 1 (Technical and Management)	IV.B.1	Required of all proposers	40 page limit
	Appendix A	IV.B.1.k	Required of all proposers	-Team member identification - Government/FFRDC team member proof of eligibility - Organizational conflict of interest affirmations - Intellectual property - Human use - Animal use - Subcontractor plan - Unpaid delinquent tax liability/felony conviction representations -CASB disclosure
	Appendix B	IV.B.1.l	Required of all proposers	Resumes are required for all team members, including subcontractors and consultants. May include links to relevant papers, reports but this is optional.
	Volume 2 (Cost)	IV.B.2	Required of all proposers	- Cover Sheet - Cost summary by year - Detailed cost information by task/month – include costs for direct labor, indirect costs/rates, materials/equipment, subcontractors/consultants, travel, other direct costs – Justification for labor costs, categories and hours - Cost spreadsheet file (.xls or equivalent format) - List of milestones for 845 OTA agreements - Subcontractor cost proposals - Consultant agreements, teaming agreements or letters of intent - Itemized list of material and equipment items to be purchased - Vendor quotes or engineering estimates for material and equipment more than $50,000 - Travel cost estimate to include purpose, departure/arrival destinations, and sample airfare -if applicable, SF 1408