Broad Agency Announcement

Open Programmable Secure 5G (OPS-5G)

HR001120S0026

January 30, 2020

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

Table of Contents

PART I: OVERVIEW INFORMATION

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

- **Funding Opportunity Title:** Open Programmable Secure 5G (OPS-5G)

- **Announcement Type:** Initial Announcement

- **Funding Opportunity Number:** HR001120S0026

- **Catalog of Federal Domestic Assistance Numbers (CFDA):**
  12.910 Research and Technology Development

- **Dates**
  - Posting Date: January 30, 2020
  - Proposal Due Date: March 17, 2020, 12:00 noon (ET)
  - Proposal Closing Date: March 17, 2020, 12:00 noon (ET)
  - Proposers Day: January 7, 2020

- **Types of Instruments that May be Awarded:** Procurement contracts, cooperative agreements or Other Transactions

- **Agency Contacts**

  - **Technical POC**: Jonathan M. Smith, Program Manager, DARPA/I2O

  - **BAA Email**: Ops-5G@darpa.mil

  - **BAA Mailing Address**:
    DARPA/I2O
    ATTN: HR001120S0026
    675 North Randolph Street
    Arlington, VA 22203-2114

  - **I2O Solicitation Website:** http://www.darpa.mil/work-with-us/opportunities

PART II: FULL TEXT OF ANNOUNCEMENT

I. Funding Opportunity Description

DARPA is soliciting innovative research proposals in the area of open source software and systems enabling secure 5G and follow-on mobile networks. 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 Federal Acquisition Regulation (FAR) 6.102(d)(2) and 35.016. Any negotiations and/or awards will use procedures under FAR 15.4 (or 32 CFR § 200.203 for grants and cooperative agreements). Proposals received as a result of this BAA shall be evaluated in accordance with evaluation criteria specified herein through a scientific review process.

DARPA posts BAAs on the System for Award Management, Contract Opportunities (Beta.Sam.Gov) website (https://beta.sam.gov/) and, when applicable, the Grants.gov website (https://www.grants.gov/).

The following information is for those wishing to respond to this BAA.

Introduction/Background
Ubiquitous mobile networking has been transformative, with impacts that pervade our daily lives. Captured data is aggregated, analyzed, and shared, typically via Internet applications using cloud computing and storage resources. Virtualization has made this approach very cost-effective.

Step	1989	2019
Contact friends	Multiple phone calls	Social network messaging
Choose restaurant	Yellow pages, local newspaper, travel guide	Consult reviews on restaurant rating web sites
Estimate travel time	Map, time of day, history	Consult online map service
Travel to restaurant	Arrange rides, etc.	Ride-sharing Application
Delayed?	Annoyance, late seating	Share with instant messaging
Seating	Stand in line	Alert with text message
Payment	Cash, check, credit card	Payment Application
Rate restaurant	Letter to manager	Post review to rating site

Table 1: Mobile Networking Transforms Lifestyles

Today, user equipment (UE) on mobile networks is dominated by smartphones, tablets, and laptops. These "edge devices" access network services such as localization on an as-needed basis. UE access to web services is via one or both of 802.11x-based WiFi and cellular. Limitations on radiated energy, shadowing and absorption by building materials, irregular deployment, and varying enterprise-specific policies limit WiFi's use as a public network.

5G[i] is the latest in a series of evolutions in public mobile networking, with widespread coverage and access on a subscription basis. 5G networks are characterized by improved capabilities across a variety of measures, including throughputs, latencies, numbers of devices, and battery life. 5G is used to attach small special purpose devices comprising the Internet of Things (IoT) to the Internet, and the important and growing number of services provided by the World Wide Web. IoT devices are often sensors, and 5G access to their data is envisioned to play important roles in medicine, manufacturing, and smart cities.

Core network features to support new applications are also present, ranging from network slicing to support for programmable networks. Support for programmability may include software-defined network (SDN)[ii] switches, network function virtualization (NFV) nodes, and many-core data plane processing devices[iii]. The combination of customized virtual infrastructures and programmability permits customization at a wide variety of network locations.

The 5G networking agenda demands massive investment, not least in infrastructure such as switches, radio equipment, real estate, swathes of provisioned radio spectrum, as well as a prodigious amount of software. Equipment vendors, mobile network operators, Internet companies, entrepreneurs, device retailers, and national governments thus have a keen focus on the evolution of the 5G network ecosystem.

Standards processes are used to maintain interoperability required for a public network, and while many of the components and component behaviors of 5G have changed little from predecessors such as 4G and LTE, the standards for the most futuristic 5G features are those most in flux[iv]. These futuristic features also present the greatest risk to US national security[v], as networks are simultaneously critical infrastructure and the means used for cyberespionage[vi] and cyberwarfare.

DARPA's Open, Programmable, Secure 5G (OPS-5G) will address this risk by pursuing research leading to development of a portable standards-compliant network stack for 5G mobile that is open source and secure by design.

Program Description/Scope
OPS-5G will create open source software and systems enabling secure 5G and subsequent mobile networks such as 6G. The signature security advantage of open source software is increased code visibility[vii][viii], meaning that code can be examined, analyzed and audited, either manually or with automated tools. In addition, the portability[ix] of open source serves, as a desired side-effect, to decouple the hardware and software ecosystems. This significantly raises the difficulty of a supply-chain attack and eases the introduction of innovative hardware into the market.

Programmability must be implemented and managed carefully[x] to achieve its potential benefits. Such benefits include bespoke networks that are tuned to application needs, as well as increased network adaptation capabilities. Programmability must also be developed in ways that avoid rampant opportunities for misuse. Ideally, the introduction of programmability for 5G will incorporate lessons learned from the well-intentioned introduction of programmability into web browsers, a capability that quickly became weaponized by malicious actors.

OPS-5G aims to improve overall 5G security. OPS-5G changes are focused on increasing trust at a set of soft points that include unmanaged, unattended, long-lived, and possibly long-forgotten

IoT devices. Additionally, OPS-5G addresses unintended and unwanted interactions between network slices and threats from the vast increases in network scale.

OPS-5G's strategic vision of mobile networking's future is shown in Figure 1.

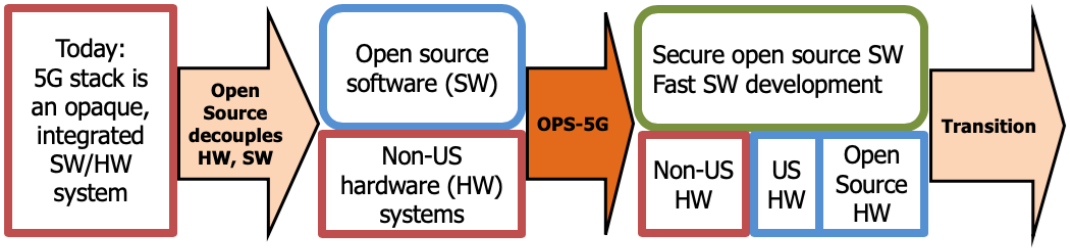

Figure 1: OPS-5G augments Open Source Software to obtain a secure 5G system (red: non-US; blue: US; green: OPS-5G)

Technical Areas and Program Structure
Challenges addressed by OPS-5G's Technical Areas (TA) are:

(1) Decreasing the time required for updates to OPS-5G open source software in response to new versions of the 5G standards;
(2) Achieving a usable scalable "zero-trust"[xi] security architecture for devices ranging from IoT sensors to servers. The architecture should have a minimal impact on size, weight and power (SWaP), and price;
(3) Mitigating new attack surfaces (such as side-channels) introduced by virtualization and slicing; and
(4) Changing programmability from a threat vector to an enabler of security at scale.

Proposers are encouraged to survey the research literature for approaches that provide differentiating value for the OPS-5G network. An example of this might use cryptographic markers or other techniques found in the network security literature to provide cryptographic proof that a path through the network was taken[xii]. Exploitation of such techniques should be explicitly identified and referenced in the proposal. Advantages of the proposed work over prior approaches as well as possible risks must be discussed.

Proposers must indicate any assumptions that may limit the applicability of their solutions. Proposers should concisely (1/2 page limit) state a "Plan B" to overcome project risks when unmet assumptions emerge.

In cases where a proposed approach requires programmability features such as network function virtualization (NFV) or software-defined networking (SDN) offered or under development by open source consortia, proposers must justify the feasibility of the deployment timeline.

As the ultimate objective for each of the technical areas (see Figure 2) is to create open-source software to be incorporated into an open source code base, any tools, methods, processes, and prototypes must be accepted by and work seamlessly in the open source 5G environment. OPS-5G performers are encouraged to view technology transition as a continuous process underway at all times during their period of performance.

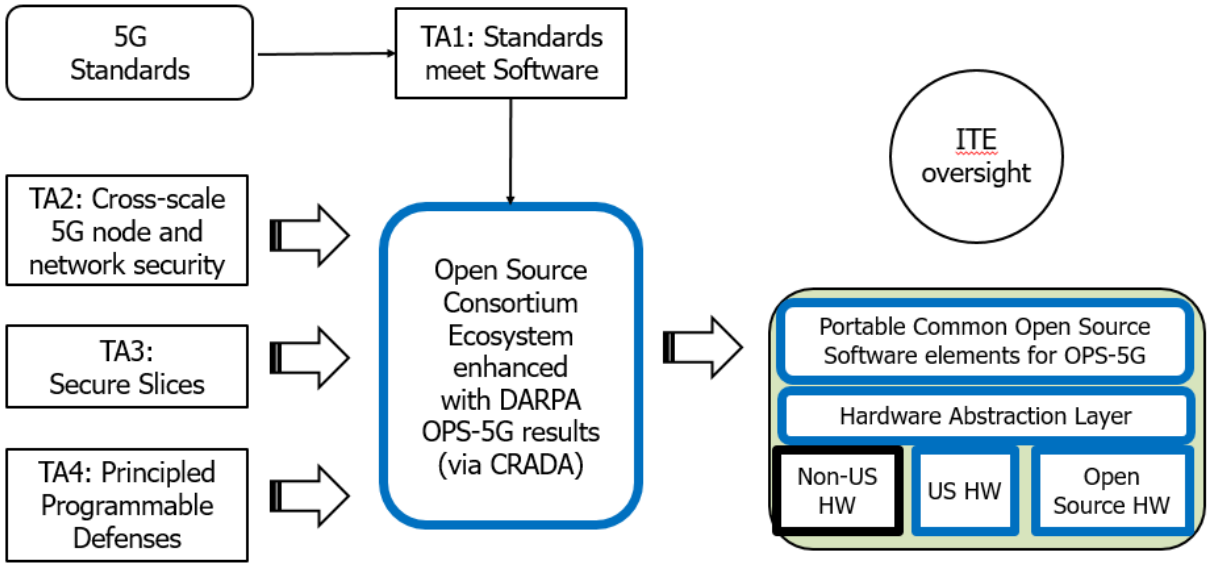

Figure 2: OPS-5G Research Results Transition to Deployable 5G Software

Proposers should detail how their research results will be inserted into typical software development processes used by an open source consortium contributing to the open source network stack. Proposers are expected to produce working prototypes that will operate within an open source consortium's ongoing 5G network development efforts.

Proposers should include time and costs for interacting with an open source consortium in their cost proposals, as the deployment of OPS-5G results via an open source consortium's networking stack is an essential element of the OPS-5G program.

Program Structure

OPS-5G is a 4-year program organized into three phases – two 18-month phases followed by a 12-month phase.

Proposals should encompass all three phases under a single, four-year effort and a nominal start date of October 1, 2020. Proposals should provide plans for iteratively developing, testing, and refining their TA1, TA2, TA3, and TA4 technologies throughout the entire four-year program.

Proposals must address only one TA, but there are no restrictions on the number of proposal submissions. Any combination of TAs (e.g., TA1 and TA4, or TA2, TA3, and TA4) may be awarded to the same proposer. If a proposer submits to multiple TAs, a discussion of the potential synergies between the proposal and the other submissions from the proposer should be included in the cost volume.

To support collaboration and the development of technology and systems in the OPS-5G program, performers will have an Associate Contractor Agreement (ACA) clause or similar language included in their award (see Section VIII.D). The ACAs are intended to ensure appropriate coordination and potential integration of work done by program performers.

Technical Area 1: Standards Meet Software

Open-source software development typically lags commercial software development because of the portable nature of open-source software, which requires the definition and software implementation of a hardware abstraction layer (HAL). This open-source versus commercial software disparity in "feature velocity" inhibits open-source software deployment in fast-paced markets (Figure 3). OPS-5G TA1 will focus on accelerating open source software development with machine translation of 5G standards documents. 5G standards are maintained online as a set of electronic documents and updated as needed. As operational 5G software must be standards compliant, updates in standards spur new software development.

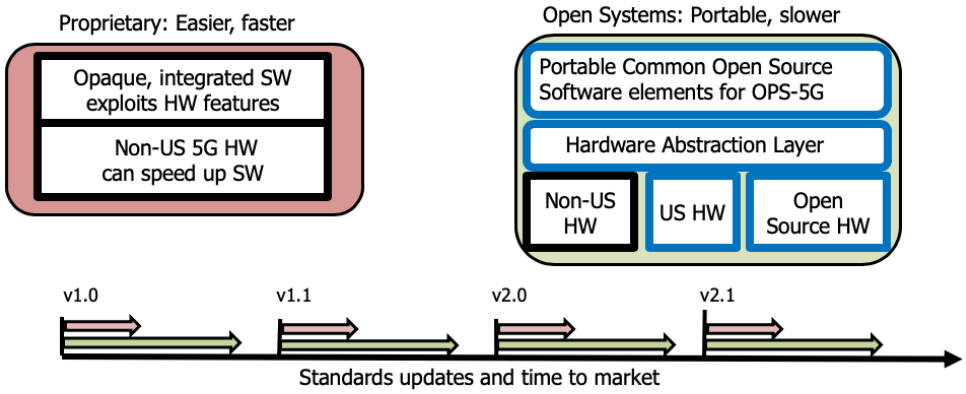

Figure 3: Today, hardware-independent open source code development often takes longer

The high degree of structure[xiii] [xiv][xv] present in these standards documents enables machine extraction of information relevant to software implementations including software structure, service interfaces, timing parameters, flow diagrams, and protocol graphs. This extracted information provides a foundation for automated compliance testing, partial proofs of correctness, protocol execution integrity checks, and other critical aspects of software development.

Accurate translation to a domain-specific intermediate form (such as frames) or a domain-specific language can feed a series of refinement steps that can accelerate production of correct software as well as improve responsiveness to standards updates. In addition to code generation, such representations are useful for tools such as theorem provers, control flow enforcement tools, compilers, etc.

The Independent Test and Evaluation (ITE) and TA1 teams will collaborate to define a sufficiently powerful and flexible formal representation for 5G standards. The ITE team will provide a ground-truth translation of these natural language documents into the representation, and TA1 performers will be evaluated on their ability to accurately translate from natural language (NL) standards documents.

Accuracy will be assessed via precision and recall as follows:

$$\text{Precision} = \frac{|\{GT\} \cap \{TA1.TeamX\}|}{|\{TA1.TeamX\}|} \qquad \text{Recall} = \frac{|\{GT\} \cap \{TA1.TeamX\}|}{|\{GT\}|}$$

where

$$|\{TA1.TeamX\}| = number\ of\ clauses\ translated\ by\ the\ TA1\ team, and$$
$$|\{GT\}| = number\ of\ clauses\ translated\ by\ the\ ITE, and$$
$$|\{GT\} \cap \{TA1.TeamX\}| =$$
$$number\ of\ matching\ ground\ truth\ and\ TA1\ team\ clauses.$$

Proposers should make clear how their process of translating or extracting information from a standards document will accelerate production of correct source code or systems elements that will contribute to a faster, more robust software infrastructure for 5G.

Capabilities of interest in TA1 include:

(1) Extracting interface descriptions used in interactions between modules and services;
(2) Extracting descriptions of interactions that describe protocols in whole or in part;
(3) Extracting parameters, such as throughputs, object sizes and delay bounds; and
(4) Extracting other features from 5G standards, such as options and error handling, when they are specified; these can be used to provide additional validation[xvi] of interactions between network elements and services that form the basis of the 5G software components in the core and mobile edge architecture.

Proposers may propose solutions that:

(1) Exploit in-network data plane processing;
(2) Result in fragments of code written in either a detailed domain specific language intended to be translated into an executable form; or
(3) Include translation directly to fragments of a target source language such as C, C++ or Java.

Other useful results related to code fragment inference are the generation of self-documenting code: generating in-line comments attached to the code fragments, along with the standards text from which the comments and code were derived. Such research may identify promising directions for further automation, such as building associations amongst code and related natural language to aid the generation of new or revised standards documents that are tightly bound to working software.

Technical Area 2: Cross-scale 5G node and network security

5G will drive substantial growth in networked devices. The size, weight, and power (SWaP) characteristics of such devices will vary tremendously, ranging from tiny battery-powered Internet of Things (IoT) sensors to substantial computing systems. The goal of TA2 is to develop techniques and security architectures enabling security at scale across devices with widely disparate SWaP.

A security architecture provides methods to preserve desired levels of confidentiality, integrity, and availability across the set of systems spanned by the architecture. On larger platforms, such

as those in the 5G core, services, protocols, hardware support, and administrative resources are available to detect and remediate problems. IoT devices, on the other hand, may be severely resource-constrained (e.g., battery-operated), cost-limited, and unattended, while meeting mission requirements for multi-year operational lifetimes. Improvements in processing time and battery life from low-cost hardware support[xvii] for security primitives such as in-silico entropy sources and encryption, as well as those required for roots of trust such as Trusted Platform Modules (TPMs)[xviii], Titan[xix], Subscriber Identity Modules (SIMs)[xx] and e-SIMs[xxi], have resulted in their presence in many microcontroller and microprocessor systems. Given needs such as trusted initialization of a node[xxii], TA2 submissions must identify hardware support presumed by their proposed solutions. If your proposal requires embedded hardware to meet OPS-5G TA2 objectives for performance and energy efficiency, it must provide comparisons of the performance versus a pure software solution, as well as estimated impacts on hardware production costs.

Adding a new, networked device[xxiii] to a household with many existing devices, such as security cameras, shows the need for cross-scale security approaches. Starting from a basis of zero trust[xxiv] ("the network cannot be trusted"), a zero trust architecture is based upon the principle of least privilege[xxvxxvi]. Roots of trust, as described above, may be used; proposers are encouraged to avoid overdependence on their presence. As trust is established amongst nodes, the network security architecture can then bind devices together using delegated authorities[xxvii] to control their roles (e.g., by not sharing security camera outputs with unauthorized users). IoT devices may be bought, sold, loaned, and relocated; thus solutions must remain secure in both long-term emplacements and in situations where trust relationships are dynamic and short-lived.

To be successful, proposers to TA2 must describe and justify security architectures that operate across all scales of nodes and networks, minimizing use of 5G core network services, and maximizing use of mobile edge computing (MEC) to avoid performance bottlenecks from shared central services. Architectures should support low-cost, unattended, long-lived, battery-powered sensors, which will be the smallest, cheapest, and most numerous devices in the 5G ecosystem. Of particular relevance are cryptographic operations, which typically demand high levels of power. The TA2 metric is cost-effective security; costs are measured using battery life relative to a baseline as a metric for SWaP. The Government will use penetration test scores devised by the Government Independent Test and Evaluation (ITE) team to gauge network and device security.

Technical Area 3: Secure slices

The performance requirements of mobile networks vary by customer and use. For example, video streaming demands completely different latency, bandwidth, and delay variability (jitter) than tele-operation. Playback of stored video can overcome the majority of timing challenges using an elastic buffer at the user device, while interactive tele-operation cannot tolerate the delays inherent in playback from a large buffer. Thus, a 5G network slice intended for content distribution must be provisioned differently than a slice used for tele-robotic surgery.

Network slicing overlays virtual networks across multiple enterprises, and thus may use infrastructure that is untrustworthy, under-provisioned or even adversarial (Figure 4). Slice virtualization security risks[xxviii] thus include timing side-channels[xxix] used to extract information from activities occurring in co-resident slices.

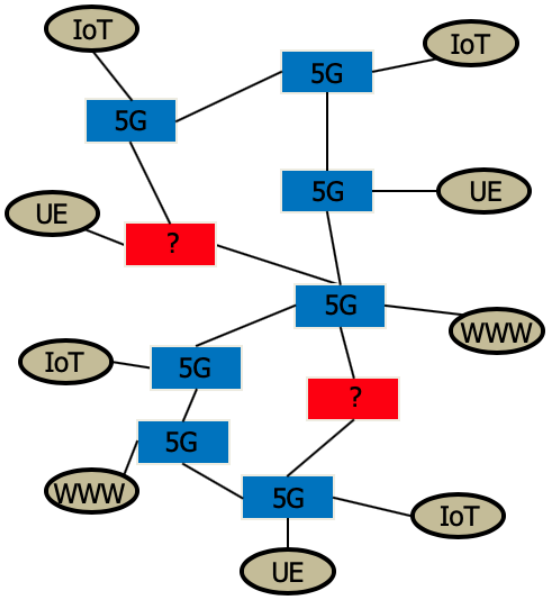

Figure 4: Network Infrastructure; Trusted (Blue), Untrusted (Red)

OPS-5G TA3 approaches can base slice-provisioning decisions on priority, soft or hard real-time capabilities at nodes, allocation of resources such as pinned memory pages, etc. System-level[xxx] and network-level slice isolation approaches include routing to minimize use of shared or untrusted resources (e.g., by purposeful route separation) as the slice is provisioned. Once policies are able to shape selection of physical components for the slice, more aggressive "moving target"-inspired periodic re-routing using programmable networks is also possible.

Assessments of integrity using remote attestation can be used in route setup or when re-routing to detect and avoid use of suspect devices. Techniques such as the ICING[xxxi] approach used in the NEBULA Future Internet Architecture[xxxii] can be used to prove an intended path was taken.

The TA3 metric is capacity. Side-channels, like covert channels, are impossible to eliminate completely. Reducing the side channel capacity is a measure of the effectiveness of performer solutions in isolating a "secure slice" from co-located slices that might be used by adversaries to extract information leaked, for example by accidental cache pollution. The capacity measure is solution-agnostic, and proposers may suggest additional metrics or milestones.

Obtaining information from a side-channel requires knowledge of its presence and a means of extracting information from it. The OPS-5G ITE team will specify the means for determining the capacity metric in bits per second (see Table 2). As an imaginative adversary might use novel or unknown methods for extracting information, ITE's assessment of the capacity metric will be limited to the benchmarks and techniques developed or adopted for use in the OPS-5G program. TA3 proposers should provide a clear and explicit threat model. The proposed solution and plan should be tied to the threat model.

TA3 proposers should make clear any assumptions about technologies provided by the other technical areas that they may have in their proposed research. For example, if particular cryptographic signature primitives are necessary for hashing or supporting challenge-response remote attestation protocols must be present in all nodes comprising a secure slice, this is a strong presumption; thus, it should be clearly and explicitly stated. Similar assumptions would

include those regarding availability and performance of cryptographic security primitives from TA2 at a selected number of nodes (e.g., the elements of a mobile edge cloud). Additional examples of such assumptions include:

(1) That awareness of node hardware provenance is available;
(2) That awareness of code bases running in the network elements may be available; or
(3) That this information is itself trustworthy (e.g., that no spoofing has occurred).

If the performance of a proposed TA3 solution depends on the availability of specific fractions of nodes with hardware roots of trust, encryption support or other technologies, this must be clearly and explicitly stated for evaluating the proposal.

TA3 approaches may also include so-called "moving target" defenses, where the network infrastructure is periodically altered as a method of blunting attacks and information extraction. If such an approach is used, proposers must clearly and explicitly state the expected effects on analysis of the capacity metric used by the ITE to evaluate TA3. For example, if a degree of redundancy in network paths is necessary for slice provisioning or re-provisioning in a TA3 solution, that expectation must be clearly stated. Measures of redundancy, such as average or minimum in-degree or out-degree for graph nodes, should be clearly and explicitly stated by proposers. Additionally, the risk if the assumption is not met must also be discussed.

TA3 proposers may build combinations of techniques; such combinations may derive their primitives from either programmability or cryptographic capabilities but should be focused on breakthrough approaches leading to secure slices.

Technical Area 4: Principled programmable defenses

Technologies such as Network Function Virtualization (NFV), Software Defined Networking (SDN), etc., allow customization of networks by injecting code on-demand to meet evolving sets of requirements. Accelerating network evolution is a central goal of OPS-5G as well. OPS-5G's ability to evolve is achieved via use and management of SDNs, NFVs, and emerging data plane capabilities.

The consequences of introducing programmability with insufficient attention to malicious actors and their capabilities is illustrated by the addition of scripting languages to web browsers. Initially intended to customize local behavior of downloaded Web content for presentation by a web browser, the execution of programs of unknown provenance has opened hosts to a multiplicity of security threats. OPS-5G's TA4, Principled programmable defenses, seeks to develop techniques that use programmability, and the resulting network adaptability, as a means to increase security. In particular, TA4 focuses on (1) innovative approaches leveraging programmability to ensure that in-network code is trustworthy; and (2) concrete demonstrations of programmable networking's advantages for network defense.

Proposers should propose novel solutions to address the challenges of:

(1) Generating and signing trustworthy code for programmability for in-line network devices;
(2) Generating and signing trustworthy code for SDN switches;

(3) Full or partial verification of code for virtual network functions (VNFs) in NFV; and
(4) Preserving integrity of the code between verification and execution.

Approaches of particular interest include:

(1) Use of programming languages and programming language techniques including strong typing, proof carrying code[xxxiii] and theorem provers;
(2) Use of system-level integrity protections[xxxiv] achieved, for example, through cryptographic operations and cryptographic protocols; and
(3) Processes for deploying new functionality in defensive nodes; these might entail use of a special purpose programming language[xxxv] and creation of tools to verify software written in a conventional programming language that can then be cryptographically signed and hashed in order to provide integrity protections.

Ultimately, the goal of TA4 is to maintain availability of the 5G infrastructure and its services in spite of active threats to its availability by malicious actors, and to use the programmable elements of the OPS-5G infrastructure to defend against compromised elements outside the control of the OPS-5G software. TA2 will provide a network security architecture that makes injection and propagation of malware within the IoT very difficult. However, devices that are not compliant with TA2's models may in fact be compromised and turned to malice, e.g., the aggregation of a titanic "botnet of things". It is such threats that TA4 solutions must defend against.

TA4 proposers should plan to design and prototype a scalable Distributed Denial of Service (DDoS) defense for 5G networks (see Table 2). Approaches to defending against DDoS attacks can include packet dropping, queuing and other techniques for policing the behavior of the network with programmable defenses. TA4 submissions may propose additional defensive applications to demonstrate the generality of a proposed approach; each additional application must be proposed as a separate extra-cost option.

Examples of additions include auxiliary protocol graphs extracted from systems that can test interactions within the distributed systems being defended. These graphs could be used to place various fault-testing code at observation points that would be embedded in the network infrastructure. For example, programmable defenses might identify themselves with cryptographic tokens and may also be used to provide an index of behavioral properties that could be used to check the application behavior as evidenced by packet flows in the network. This class of approach has the virtue that it can be used for self-checking and in addition, detection of malicious behavior.

TA4 proposals must include a specific demonstration of the efficacy of the proposed general approach to exploiting programmability as a defensive capability. TA4 proposals must include plans to evaluate proposed solutions on a challenge problem, namely countering large botnets via elision of their connectivity.

A botnet comprises a set of compromised machines ("bots") under the control of a "botmaster". The Mirai botnet is distinguished by its exploitation and use of IoT devices as bots. At its peak size of an estimated 600K nodes, Mirai delivered crippling DDoS attacks, with 623 Gbps of packet traffic directed against a target server.

In light of this, the vast increase in IoT devices connected via 5G represents a significant threat. While the technologies developed under TA2 will inhibit bot recruitment, IoT devices independent of OPS-5G will remain subject to compromise at scale. TA4 technologies will enable scalable resilience by detecting the onset of DDoS attacks with in-network sensors and deploying active in-network defenses[xxxvi] in response. Proposers should plan to prototype capabilities sufficient to meet program metrics for the scale of DDoS attacks generated by large pools of IoT nodes as exemplified by the Mirai botnet[xxxvii].

The TA4 metric is latency at scale, to measure the ability to rapidly detect threats, determine appropriate defenses, and deploy and actuate these defenses against an adaptive adversary operating at scale. Latency measures the ability of the defender to adapt and dominate an adaptive adversary using the principles of John Boyd's "Observe Orient Decide Act" (OODA) Loop. OPS-5G scalability milestones are designed so that botnet reaction velocity goals remain extremely aggressive as the number of 5G devices expands throughout the course of the program.

TA4 proposers should describe their approach for achieving TA4 metrics for Phases 1, 2, and 3. This must include description of a simulator or emulator (e.g., Mininet[xxxviii]) that permits architectural features such as programmability in the edge or caching in the edge to be modeled. TA4 performers will be able to evolve their evaluation environments over the course of the program in response to guidance provided by the OPS-5G ITE team. The ITE team will validate TA4 performer's evaluations at TA4 performer sites, using TA4 performer facilities.

TA4 proposers should indicate any cryptographic requirements presumed available in the proposed approach (e.g., cryptographic hashes needed for secure bootstrap) and if needed, where these capabilities reside, e.g., in OPS-5G TA2 IoT devices or elsewhere in the environment where code is executing. Any assumptions about availability and timing of results from the other OPS-5G technical areas must be explicitly stated in TA4 submissions. TA4 proposers must explicitly state any and all assumptions made about the availability of programmable infrastructures needed for their solutions such as where 5G mobile edge computing (MEC) or other edge clouds are in the architecture. Any requirements that must be known to the ITE to evaluate proposed systems must be specified clearly and explicitly in TA4 proposals. Research prototypes must operate in the network programmability frameworks provided by an open source consortium. This is necessary to validate real-world deployment of OPS-5G.

Experimental validation of moderate-scale realizations of TA4 solutions at the end of Phase 2 requires software deliverables (e.g., for Virtual Network Functions) that operate in an OPS-5G evaluation environment to be defined by the ITE team. The ITE team will evaluate TA4 realizations on US Government facilities. Therefore, TA4 proposals must not replicate independent testbeds at program scale (10,000 nodes).

Schedule/Milestones
OPS-5G is a 4-year program organized into three phases:

- Phase 1 (18 months): During this phase, OPS-5G will develop the initial capabilities at performance levels (see Table 2) required for the four OPS-5G technical areas described in this document. DARPA management is initiating a relationship with an open source consortium to enable transition efforts. During this phase, performers will continue to develop this relationship, which includes adoption of an appropriate integrated code and documentation delivery process, and support of other developers as needed. The end of phase milestone for the program will be a functioning demonstration of voice telephony between the DARPA Conference Center (DCC) in Arlington, Virginia and the USD(R&E) 5G test site at NIWC Pacific.

- Phase 2 (18 months): This phase will focus on maturing the capabilities demonstrated in Phase 1 to meet performance levels (see Table 2) for the four OPS-5G technical areas. The end of phase milestone will be a demonstration of data collected from 1,000 or more devices delivered over an OPS-5G slice operating over untrusted hardware. The demonstration will transfer data from the devices to infrastructure at the DARPA Conference Center for real-time analysis and display.

- Phase 3 (12 months): This phase finalizes the maturation of the capabilities developed in Phase 2, and achieves the end of program performance levels (see Table 2) for the four OPS-5G technical areas. The end of program milestone is commercial availability of the OPS-5G stack in at least one mobile network operator and in user equipment as appropriate.

	Phase 1 (18 months)	**Phase 2 (18 months)**	**Phase 3 (12 months)**
TA1 Accuracy as precision and recall	60% precision and recall, ITE-chosen document	80% precision and recall, ITE-chosen document	95% precision and recall ITE-chosen document
TA2 Security and SWaP	256-bit “encrypt & sign” in < 10 sec using < 70% battery	Resist ITE penetration test of many-to-many IoT for 4 hours using < 50% battery	Resist ITE penetration test on 10K IoT + UE for 2 days using < 25% battery
TA3 Secure slice timing channel capacity	3x reduction in timing channel capacity	10x reduction in timing channel capacity	50x reduction in timing channel capacity
TA4 Mirai botnet DDoS mitigation time	60 seconds 1G emulated nodes	1 second 10K distributed IoT nodes	60 seconds 1T emulated nodes

	Phase 1 (18 months)	Phase 2 (18 months)	Phase 3 (12 months)
Milestone Demonstrations	Secure voice call between DARPA Conference Center (DCC) and USD(R&E) 5G test site at NIWC Pacific.	Data from 1K devices to DCC over untrusted hardware from USD(R&E) 5G test site at NIWC Pacific and other sites.	Commercial availability in User Equipment (UE) and at least 1 US mobile network operator.

Table 2: Program Metrics by Phase and Technical Area (TA)

Program Meetings

DARPA will conduct frequent meetings, workshops, and demonstration events throughout the OPS-5G program. For cost estimation purposes, assume that the locations for all meetings will alternate between San Diego, CA, and Washington, DC unless specified otherwise below.

Biannual Principal Investigator (PI) meetings and biannual development workshops will be held throughout the OPS-5G program. The Program Manager will assess progress at PI meetings via performer briefings and technical exchanges along with input from the USG ITE. Performers will be expected to demonstrate their individual projects at every PI meeting. The development workshops will be held to facilitate integration efforts across the program. Anticipate the duration of PI meetings to be 2 days and development workshops to be 1 day.

One-day program summits will be held at the same location immediately following the PI meetings. The OPS-5G program uses these invitation-only summits to drive interaction amongst OPS-5G performers, mobile network operators, infrastructure and device vendors, DoD and other government components such as the Department of State, the Intelligence Community, the Department of Homeland Security, and the Federal Communications Commission. Demonstrations will be held at summits.

Formal program evaluations, including integrated system demonstrations, will be conducted by the Government team at the conclusion of each phase at DARPA and are expected to last one day each.

The program schedule and milestones are shown in Table 3.

	Phase 1												Phase 2						Phase 3					
Government Fiscal Year	2020		2021						2022						2023				2024					
Program Month	2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48
PI Meetings	♦			♦			♦			♦			♦			♦			♦			♦		
Development Workshops		♦			♦			♦			♦			♦			♦			♦			♦	
Program Summits				♦			♦			♦			♦			♦			♦			♦		♦
Program Evaluations												♦						♦						♦
Project Demos				♦			♦			♦			♦			♦			♦			♦		
Integrated System Demos												♦						♦						♦

Table 3: OPS-5G Schedule and Milestones

Deliverables
All performers will be required to provide the following deliverables:

- All technical documents and products derived from work funded by this program;
- Annotated slide presentations must be delivered within one month after each PI meeting, development workshop or other program event;
- Quarterly technical status reports detailing progress made, tasks accomplished, major risks, planned activities, trip summaries, changes to key personnel any potential issues of problem areas that require the attention of the government team these must be part provided within 15 days of the end of each quarter;
- Monthly financial status reports must be provided within 15 days of the end of each calendar month;
- A final phase report for each program phase that concisely summarizes the effort conducted, technical achievements, and remaining technical challenges will be due 30 days after the end of each phase; and
- A final report at the end of the overall period of performance that summarizes the project.

The Government desires the following deliverables:

- Commented source code, delivered in a form and with licensing acceptable to an open source consortium;
- All other necessary data, build scripts, and documentation including at a minimum user manuals and a detailed software design document for all software developed under this program.

Government-furnished Property/Equipment/Information
None.

Intellectual Property
The OPS-5G program will emphasize creating and leveraging open source technology and architectures. Clarity is of the utmost importance regarding these rights assertions, as a key goal of the OPS-5G program is establishing an open standards-based, multisource plug-and-play mobile networking architecture that allows for an unprecedented degree of interoperability and integration. This includes the ability to easily add, remove, substitute, and modify software and hardware components. This will facilitate rapid innovation by providing a base for future users or developers to use OPS-5G program technologies and deliverables in their products and networks.

The Government desires for all work products and deliverables produced by OPS-5G program efforts, such as software, documentation and generated technical data be provided with a license and rights acceptable to an open source consortium. Any lesser rights may adversely impact the intended goals of the program and thus will be carefully examined as part of the review process.

II. Award Information

A. Awards

DARPA anticipates multiple awards for each of TA1, TA2, TA3, and TA4.

The level of funding for individual awards made under this solicitation has not been predetermined and will depend on the quality of the proposals received and the availability of funds.

The Government will select for award proposals which are determined to be the most advantageous to the Government, all factors considered, including the potential contributions of the proposed work, overall funding strategy, and availability of funding. See Section V for further information.

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 with proposers 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 increments and/or with options for continued work at the end of one or more phases;
- request additional documentation once the award instrument has been determined (e.g., representations and certifications); and
- 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.

Proposals selected for award negotiation may result in a procurement contract, cooperative agreement, or Other Transaction (OT) depending upon the nature of the work proposed, the required degree of interaction between parties, and other factors. Grants will NOT be awarded under this program.

Proposers looking for innovative, commercial-like contractual arrangements are encouraged to consider requesting Other Transactions. To understand the flexibility and options associated with Other Transactions, consult http://www.darpa.mil/work-with-us/contract-management#OtherTransactions.

In accordance with 10 U.S.C. § 2371b(f), the Government may award a follow-on production contract or Other Transaction (OT) for any OT awarded under this BAA if: (1) that participant in the OT, or a recognized successor in interest to the OT, successfully completed the entire prototype project provided for in the OT, as modified; and (2) the OT provides for the award of a follow-on production contract or OT to the participant, or a recognized successor in interest to the OT.

In all cases, the Government contracting officer shall have sole discretion to select award instrument type, regardless of instrument type proposed, and to negotiate all instrument terms

and conditions with selectees. DARPA will apply publication or other restrictions, as necessary, if it determines that the research resulting from the proposed effort will present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Any award resulting from such a determination will include a requirement for DARPA permission before publishing any information or results on the program. For more information on publication restrictions, see the section below on Fundamental Research.

B. Fundamental Research

It is DoD policy that the publication of products of fundamental research will remain unrestricted to the maximum extent possible. National Security Decision Directive (NSDD) 189 defines fundamental research as follows:

> 'Fundamental research' means basic and applied research 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.

As of the date of publication of this BAA, the Government expects that program goals as described herein may be met by proposed efforts for fundamental research and non-fundamental research. Some proposed research may present a high likelihood of disclosing performance characteristics of military systems or manufacturing technologies that are unique and critical to defense. Based on the anticipated type of proposer (e.g., university or industry) and the nature of the solicited work, the Government expects that some awards will include restrictions on the resultant research that will require the awardee to seek DARPA permission before publishing any information or results relative to the program.
Proposers should indicate in their proposal whether they believe the scope of the research included in their proposal is fundamental or not. While proposers should clearly explain the intended results of their research, the Government shall have sole discretion to determine whether the proposed research shall be considered fundamental and to select the award instrument type. Appropriate language will be included in resultant awards for non-fundamental research to prescribe publication requirements and other restrictions, as appropriate. This language can be found at http://www.darpa.mil/work-with-us/additional-baa.

For certain research projects, it may be possible that although the research to be performed by a potential awardee is non-fundamental research, its proposed subawardee's effort may be fundamental research. It is also possible that the research performed by a potential awardee is fundamental research while its proposed subawardee's effort may be non-fundamental research. In all cases, it is the potential awardee's responsibility to explain in its proposal which proposed efforts are fundamental research and why the proposed efforts should be considered fundamental research.

C. Disclosure of Information and Compliance with Safeguarding Covered Defense Information Controls

The following provisions and clause apply to all solicitations and contracts; however, the definition of "controlled technical information" clearly exempts work considered fundamental

research and therefore, even though included in the contract, will not apply if the work is fundamental research.

DFARS 252.204-7000, “Disclosure of Information”
DFARS 252.204-7008, “Compliance with Safeguarding Covered Defense Information Controls”
DFARS 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting”

The full text of the above solicitation provision and contract clauses can be found at http://www.darpa.mil/work-with-us/additional-baa#NPRPAC.

Compliance with the above requirements includes the mandate for proposers to implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations” (see https://doi.org/10.6028/NIST.SP.800-171r1) that are in effect at the time the BAA is issued.

For awards where the work is considered fundamental research, the contractor will not have to implement the aforementioned requirements and safeguards. However, should the nature of the work change during performance of the award, work not considered fundamental research will be subject to these requirements.

III. Eligibility Information

A. Eligible Applicants

DARPA welcomes engagement from all responsible sources capable of satisfying the Government's needs, including academia (colleges and universities); businesses (large, small, small disadvantaged, etc.); other organizations (including non-profit); other entities (foreign, domestic, and government); FFRDCs; minority institutions; and others.

DARPA welcomes engagement from non-traditional sources in addition to current DARPA performers.

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

a. FFRDCs

FFRDCs are subject to applicable direct competition limitations and cannot propose to this BAA in any capacity unless they meet the following conditions. (1) FFRDCs must clearly demonstrate that the proposed work is not otherwise available from the private sector. (2) FFRDCs must provide a letter, on official letterhead from their sponsoring organization, that (a) cites the specific authority establishing their eligibility to propose to Government solicitations and compete with industry, and (b) certifies the FFRDC's compliance with the associated FFRDC sponsor agreement's terms and conditions. These conditions are a requirement for FFRDCs proposing to be awardees or subawardees.

b. Government Entities

Government Entities (e.g., Government/National laboratories, military educational institutions, etc.) are subject to applicable direct competition limitations. Government Entities must clearly demonstrate that the work is not otherwise available from the private sector and provide written documentation citing the specific statutory authority and contractual authority, if relevant, establishing their ability to propose to Government solicitations and compete with industry. This information is required for Government Entities proposing to be awardees or subawardees.

c. Authority and Eligibility

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 FFRDC and Government Entity eligibility submissions on a case-by-case basis; however, the burden to prove eligibility for all team members rests solely with the proposer.

2. Foreign Participation

Non-U.S. organizations and/or individuals 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. Organizational Conflicts of Interest

FAR 9.5 Requirements

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

Agency Supplemental OCI Policy

In addition, DARPA has a supplemental OCI policy that prohibits contractors/performers from concurrently providing Scientific Engineering Technical Assistance (SETA), Advisory and Assistance Services (A&AS) or similar support services and being a technical performer. Therefore, as part of the FAR 9.5 disclosure requirement above, a proposer must affirm whether the proposer or *any* proposed team member (subawardee, consultant) is providing SETA, A&AS, or similar support to any DARPA office(s) under: (a) a current award or subaward; or (b) a past award or subaward that ended within one calendar year prior to the proposal's submission date.

If SETA, A&AS, or similar support is being or was provided to any DARPA office(s), the proposal must include:

- The name of the DARPA office receiving the support;
- The prime contract number;
- Identification of proposed team member (subawardee, consultant) providing the support; and
- An OCI mitigation plan in accordance with FAR 9.5.

Government Procedures

In accordance with FAR 9.503, 9.504 and 9.506, the Government will evaluate OCI mitigation plans to avoid, neutralize or mitigate potential OCI issues before award and to determine whether it is in the Government's interest to grant a waiver. The Government will only evaluate OCI mitigation plans for proposals that are determined selectable under the BAA evaluation criteria and funding availability.

The Government may require proposers to provide additional information to assist the Government in evaluating the proposer's OCI mitigation plan.

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

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., OTs under the authority of 10 U.S.C. § 2371).

IV. Application and Submission Information

A. Address to Request Application Package

This document contains all information required to submit a response to this solicitation. No additional forms, kits, or other materials are needed except as referenced herein. No request for proposal (RFP) or additional solicitation regarding this opportunity will be issued, nor is additional information available except as provided at the System for Award Management, Contract Opportunities website (https://beta.sam.gov), the Grants.gov website (https://www.grants.gov/), or referenced herein.

B. Content and Form of Application Submission

1. Proposals

Proposals consist of Volume 1: Technical and Management Proposal (including mandatory Appendix A and optional Appendix B); Volume 2: Cost Proposal; the Level of Effort Summary by Task Excel spreadsheet; and the PowerPoint summary slide.

All pages shall be formatted for printing on 8-1/2 by 11-inch paper with 1-inch margins, single-line spacing, and 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. All pages of Volume 1 should be numbered.

A summary slide of the proposed effort, in PowerPoint format, should be submitted with the proposal. A template slide is provided as an attachment to the BAA. Submit this PowerPoint file in addition to Volumes 1 and 2 of your full proposal, and the Level of Effort Summary by Task Excel spreadsheet. This summary slide does not count towards the total page count.

Reminder – Each proposal submitted in response to this BAA shall address only one TA. Organizations may submit multiple proposals to any one TA, or they may propose to multiple TAs.

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

a. Volume 1: Technical and Management Proposal

The maximum page 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 optional. Additional information not explicitly called for here must not be submitted with the proposal, but may be included in the bibliography in Appendix B. Such materials will be considered for the reviewers' convenience only and not evaluated as part of the proposal.

Volume 1 must include the following components:

i. Cover Sheet: Include the following information.

- Label: "Proposal: Volume 1"
- BAA number (HR001120S0026)
- Technical Area
- Proposal title
- Lead organization (prime contractor) name
- Type of organization, selected from the following categories: Large Business, Small Disadvantaged Business, Other Small Business, HBCU, MI, Other Educational, or Other Nonprofit
- Technical point of contact (POC) including name, mailing address, telephone number, and email address
- Administrative POC including name, mailing address, telephone number, and email address
- Award instrument requested: procurement contract (specify type), cooperative agreement or OT.[1]
- Total amount of the proposed effort
- Place(s) and period(s) of performance
- Other team member (subcontractors and consultants) information (for each, include Technical POC name, organization, type of organization, mailing address, telephone number, and email address)
- Proposal validity period (minimum 120 days)
- Data Universal Numbering System (DUNS) number[2]
- Taxpayer Identification Number (TIN)[3]
- Commercial and Government Entity (CAGE) code[4]
- Proposer's reference number (if any)

ii. Table of Contents

iii. Innovative Claims and Deliverables: Describe the innovative aspects of the project in the context of existing capabilities and approaches, clearly delineating the uniqueness

[1] Information on award instruments can be found at http://www.darpa.mil/work-with-us/contract-management.
[2] The DUNS number is used as the Government's contractor identification code for all procurement-related activities. Go to http://fedgov.dnb.com/webform/index.jsp to request a DUNS number (may take at least one business day). For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa for further information.
[3] See http://www.irs.gov/businesses for information on requesting a TIN. Note, requests may take from 1 business day to 1 month depending on the method (online, fax, mail).
[4] A CAGE Code identifies companies doing or wishing to do business with the Federal Government. For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa.

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.

iv. 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.

v. Management Plan: Provide a summary of expertise of the proposed team, including any subcontractors/consultants and key personnel who will be executing the work. Resumes count against the proposal page limit so proposers may wish to include them in Appendix B below. Identify a principal investigator (PI) 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. List Government-furnished materials or data assumed to be available.

vi. Personnel, Qualifications, and Commitments: List key personnel (no more than one page per person), showing a concise summary of their qualifications, discussion of previous accomplishments, and work in this or closely related research areas. Indicate the level of effort in terms of hours to be expended by each person during each contract year and other (current and proposed) major sources of support for them and/or commitments of their efforts. DARPA expects all key personnel associated with a proposal to make a substantial time commitment to the proposed activity and the proposal will be evaluated accordingly. It is DARPA's intention to put key personnel conditions into the awards, so proposers should not propose personnel that are not anticipated to execute the award.

Include a table of key individual time commitments as follows:

Key Individual	Project	Status (Current, Pending, Proposed)	Hours on Project		
			Phase 1	Phase 2	Phase 3
Name 1	**Program name**	Proposed	x	x	X
	Project Name 1	Current	x	x	n/a
	Project Name 2	Pending	n/a	x	X
Name 2	**Program Name**	Proposed	x	x	X
	Project Name 3	Proposed	x	x	X

vii. Capabilities: Describe organizational experience in relevant subject area(s), existing intellectual property, or specialized facilities. Discuss any work in closely related research areas and previous accomplishments.

viii. Statement of Work (SOW): The SOW must provide a detailed task breakdown, citing specific tasks and their connection to the interim milestones and 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(s), consultant(s)), by name.
- A measurable milestone, (e.g., a deliverable, demonstration, or other event/activity that marks task completion).
- A definition of all deliverables (e.g., data, reports, software) to be provided to the Government in support of the proposed tasks/subtasks.
- Identify any tasks/subtasks (by the prime or subcontractor) that will be accomplished at a university and believed to be fundamental research.

ix. 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 the project.

x. Level of Effort Summary by Task: Provide a one-page table summarizing estimated level of effort per task (in hours) broken out by senior, mid-level and junior personnel, in the format shown below in Figure 2. Also include dollar-denominated estimates of travel, materials and equipment. For this table, consider materials to include the cost of any data sets or software licenses proposed. For convenience, an Excel template is available for download along with the BAA. This summary slide does not count towards the total page count.

SOW Task		Duration (months)	Labor Hours						
			Senior	Mid	Junior	Total	SubC	Conslt	Total
1.1.0	<Phase 1 Task 1 name>	7	*240*	*680*	*24*	*944*	-	*200*	**944**
1.1.1	<Subtask 1.1.1 name>	4	80	280	-	360	-	200	**360**
1.1.2	<Subtask 1.1.2 name>	3	160	400	24	584	-	-	**584**
1.2.0	<Phase 1 Task 2 name>	6	*108*	*400*	*1,800*	*2,308*	*1,400*	-	**3,708**
1.2.1	<Subtask 1.2.1 name>	3	48	320	1,600	1,968	600	-	**2,568**
1.2.2	<Subtask 1.2.2 name>	3	60	80	200	340	800	-	**1,140**
:	:	:	:	:	:	:	:	:	:
	Phase 1 Total Hours	**16**	**348**	**1,080**	**1,824**	**3,252**	**1,400**	**200**	**4,652**
Phase 1	Travel	$ 44,000					$12,000	$2,000	*$ 58,000*
Costs	Materials & Equipment	$ 8,000					$ -	$ -	*$ 8,000*
2.1.0	<Phase 2 Task 1 name>	8	*176*	*560*	*64*	*800*	*100*	*100*	**900**
2.1.1	<Subtask 2.1.1 name>	7	96	240	24	360	100	100	**460**
2.1.2	<Subtask 2.1.2 name>	4	80	320	40	440	-	-	**440**
2.2.0	<Phase 2 Task 2 name>	6	*180*	*520*	*1,800*	*2,500*	*1,240*	-	**3,740**
2.2.1	<Subtask 2.2.1 name>	4	140	400	1,200	1,740	400	-	**2,140**
2.2.2	<Subtask 2.2.2 name>	4	40	120	600	760	840	-	**1,600**
:	:	:	:	:	:	:	:	:	:
	Phase 2 Total Hours	**16**	**356**	**1,080**	**1,864**	**3,300**	**1,340**	**100**	**4,640**
Phase 2	Travel	$ 48,000					$13,000	$2,400	*$ 63,400*
Costs	Materials & Equipment	$ -					$ -	$ -	*$ -*
3.1.0	<Phase 3 Task 1 name>	9	*120*	*400*	*120*	*640*	*100*	*100*	**740**
3.1.1	<Subtask 3.1.1 name>	3	40	200	40	*280*	100	100	**380**
3.1.2	<Subtask 3.1.2 name>	6	80	200	80	*360*	-	-	**360**
3.2.0	<Phase 3 Task 2 name>	6	*160*	*800*	*1,800*	*2,760*	*1,200*	-	**3,960**
3.2.1	<Subtask 3.2.1 name>	4	80	400	1,000	*1,480*	600	-	**2,080**
3.2.2	<Subtask 3.2.2 name>	3	80	400	800	*1,280*	600	-	**1,880**
:	:	:	:	:	:	:	:	:	:
	Phase 3 Total Hours	**16**	**280**	**1,200**	**1,920**	**3,400**	**1,300**	**100**	**4,700**
Phase 3	Travel	$ 49,000					$12,000	$2,000	*$ 63,000*
Costs	Materials & Equipment	$ -					$ -	$ -	*$ -*
	Project Total Hours	**48**	**984**	**3,360**	**5,608**	**9,952**	**4,040**	**400**	**13,992**
Project	Travel	**$141,000**					**$37,000**	**$6,400**	***$ 184,400***
Costs	Materials & Equipment	**$ 8,000**					**$ -**	**$ -**	***$ 8,000***

x. Appendix A: This section is mandatory and must include all of the following components. If a particular subsection is not applicable, state "NONE". There is no page limit on Appendix A.

(1). Team Member Identification: Provide a list of all team members including the prime, subcontractor(s), and consultant(s), as applicable. Identify specifically whether any are a non-US organization or individual, FFRDC and/or Government entity. Use the following format for this list:

Individual Name	Role (Prime, Subcontractor or Consultant)	Organization	Non-US?		FFRDC or Govt?
			Org	Ind.	

(2). Government or FFRDC Team Member Proof of Eligibility to Propose: 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.1) citing the specific authority that establishes the applicable team member's eligibility 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.

(3). 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 (per Section III.A.1) that demonstrates the work to be performed by the Government entity or FFRDC team member is not otherwise available from the private sector.

(4). Organizational Conflict of Interest Affirmations and Disclosure: If none of the proposed team members is currently providing SETA or similar support as described in Section III.B, state "NONE".

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

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

(5). Intellectual Property (IP): If no IP restrictions are intended, state "NONE". The Government will assume unlimited rights to all IP not explicitly identified as

having less than unlimited rights in the proposal.

For all noncommercial technical data or computer software that will be furnished to the Government with other than unlimited rights, provide (per Section VI.B.1) 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. Use the following format for these lists:

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)
(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)
(List)	(Narrative)	(List)	(List)	(List)

(6). Human Subjects Research (HSR): If HSR is not a factor in the proposal, state "NONE".

If the proposed work will involve human subjects, provide evidence of or a plan for review by an Institutional Review Board (IRB). For further information on this subject, see Section VI.B.2.

(7). Animal Use: If animal use is not a factor in the 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.2.

(8). Representations Regarding Unpaid Delinquent Tax Liability or a Felony Conviction under Any Federal Law: For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa.

Please also complete the following statements.

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

(9). Cost Accounting Standards (CAS) Notices and Certification: For any proposer who submits a proposal which, if accepted, will result in a CAS-compliant contract, must include a Disclosure Statement as required by 48 CFR 9903.202. The disclosure forms may be found at https://www.whitehouse.gov/wp-content/uploads/2017/11/CASB_DS-1.pdf

If this section is not applicable, state "NONE". For further information regarding this subject, please see www.darpa.mil/work-with-us/additional-baa.

xii. Appendix B: If desired, include a brief bibliography to relevant papers, reports, or resumes. Do not include technical papers. This section is optional, and the materials will not be evaluated as part of the proposal review.

b. Volume 2 - Cost Proposal

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

The cost proposal should include a working spreadsheet file (.xls, .xlsx or equivalent format) that provides formula traceability among all components of the cost proposal. The spreadsheet file should be included as a separate component of the full proposal package. Costs must be traceable between the prime and subcontractors/consultants, as well as between the cost proposal and the SOW.

Pre-award costs will not be reimbursed unless a pre-award cost agreement is negotiated prior to award.

i. Cover Sheet: Include the same information as the cover sheet for Volume 1, but with the label "Proposal: Volume 2."

ii. Cost Summary Tables: Provide a single-page summary table broken down by fiscal year listing cost totals for labor, materials, other direct charges (ODCs), indirect costs (overhead, fringe, general and administrative [G&A]), and any proposed fee for the project. Include costs for each task in each fiscal year of the project by prime and major subcontractors, total cost and proposed cost share, if applicable. Provide a second table containing the same information broken down by project phase.

iii. Cost Details: For each task, provide the following cost details by month. Include supporting documentation describing the method used to estimate costs. Identify any cost sharing.

(1) Direct Labor: Provide labor categories, rates and hours. Justify rates by providing examples of equivalent rates for equivalent talent, past commercial or Government rates from a Government audit agency such as the Defense

Contract Audit Agency (DCAA), the Office of Naval Research (ONR), the Department of Health and Human Services (DHHS), etc.

(2) Indirect Costs: Identify all indirect cost rates (such as fringe benefits, labor overhead, material overhead, G&A or F&A, etc.) and the basis for each.

(3) Materials: Provide an itemized list of all proposed materials, equipment, and supplies for each year including quantities, unit prices, proposed vendors (if known), and the basis of estimate (e.g., quotes, prior purchases, catalog price lists, etc.). For proposed equipment/information technology (as defined in FAR 2.101) purchases equal to or greater than $50,000, include a letter justifying the purchase. Include any requests for Government-furnished equipment or information with cost estimates (if applicable) and delivery dates.

(4) Travel: Provide a breakout of travel costs including the purpose and number of trips, origin and destination(s), duration, and travelers per trip.

(5) Subcontractor/Consultant Costs: Provide above information for each proposed subcontractor/consultant. Subcontractor cost proposals must include interdivisional work transfer agreements or similar arrangements. If the proposer has conducted a cost or price analysis to determine reasonableness, submit a copy of this along with the subcontractor proposal.

The proposer is responsible for the compilation and submission of all subcontractor/consultant cost proposals. At a minimum, the submitted cost volume must contain a copy of each subcontractor or consultant non-proprietary cost proposal (i.e. cost proposals that do not contain proprietary pricing information such as rates, factors, etc.). Proprietary subcontractor/consultant cost proposals may be included as part of Volume 2. Proposal submissions will not be considered complete unless the Government has received all subcontractor/consultant cost proposals.

If proprietary subcontractor/consultant cost proposals are not included as part of Volume 2, they may be emailed separately to OPS-5G@darpa.mil. Email messages must include "Subcontractor Cost Proposal" in the subject line and identify the principal investigator, prime proposer organization and proposal title in the body of the message. Any proprietary subcontractor or consultant proposal documentation which is not uploaded to the DARPA BAA Submission Website as part of the proposer's submission or provided by separate email shall be made immediately available to the Government, upon request, under separate cover (i.e., mail, electronic/email, etc.), either by the proposer or by the subcontractor/consultant organization.

Please note that a ROM or similar budgetary estimate is not considered a fully qualified subcontract cost proposal submission. Inclusion of a ROM or similar budgetary estimate, or failure to provide a subcontract proposal, may result in the full proposal being deemed non-compliant.

(6) Other Direct Costs (ODCs): Provide an itemized breakout and explanation of all anticipated ODCs.

iv. Proposals Requesting a Procurement Contract: Provide the following information where applicable.

(1) Proposals exceeding the Certification of Cost or Pricing Threshold: Provide "certified cost or pricing data" (as defined in FAR 2.101) or a request for exception in accordance with FAR 15.403.

(2) Proposals for $700,000 or more: 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. In accordance with FAR 19.702(a)(1) and 19.702(b), prepare a subcontractor plan, if applicable. The plan format is outlined in FAR 19.704.

(3) Proposers without an adequate cost accounting system: If requesting a cost-type contract, provide the DCAA Pre-award Accounting System Adequacy Checklist to facilitate DCAA's completion of an SF 1408. Proposers without an accounting system considered adequate for determining accurate costs must complete an SF 1408 if a cost type contract is to be negotiated. To facilitate this process, proposers should complete the SF 1408 found at http://www.gsa.gov/portal/forms/download/115778 and submit the completed form with the proposal. To complete the form, check the boxes on the second page, then provide a narrative explanation of your accounting system to supplement the checklist on page one.

v. Proposals Requesting an Other Transaction: Proposers must indicate whether they qualify as a nontraditional Defense contractor[5], have teamed with a nontraditional Defense contractor, or are providing a one-third cost share for this effort. Provide information to support the claims.

Provide a detailed list of milestones including: description, completion criteria, due date, and payment/funding schedule (to include, if cost share is proposed, contractor and Government share amounts). Milestones must relate directly to accomplishment of technical metrics as defined in the solicitation and/or the proposal. While agreement type (fixed price or expenditure based) will be subject to negotiation, the use of fixed price milestones with a payment/funding schedule is preferred. Proprietary information must not be included as part of the milestones.

[5] For definitions and information on an OT agreement see http://www.darpa.mil/work-with-us/contract-management..

c. Level of Effort Summary by Task Spreadsheet

Provide a one-page table summarizing estimated level of effort per task (in hours) broken out by senior, mid-level, and junior personnel, in the format shown below in Figure 4. Also include dollar-denominated estimates of travel, materials, and equipment. For this table, consider materials to include the cost of any data sets or software licenses proposed. For convenience, an Excel template is available for download along with the BAA. Submit the Level of Effort Summary Excel file (do not convert the Excel file to pdf format) in addition to Volume 1 and Volume 2 of your full proposal. This Excel file does not count towards the total page count.

SOW Task		Duration (months)	Intensity (hrs/mo)	Labor Hours for Prime							Labor Hours for Subcontractor/Consultants							
				Sr	Skill set(s)	Mid	Skill set(s)	Jr	Skill set(s)	Total	SubC-Sr	Skill set(s)	SubC-Mid	Skill set(s)	SubC-Jr	Skill set(s)	Conslt	Total
1.1.0	<Phase 1 Task 1 name>	7	135	240		680		24		944	-						200	1,144
1.1.1	<Subtask 1.1.1 name>	4	90	80		280		-		360	-						200	560
1.1.2	<Subtask 1.1.2 name>	3	195	160		400		24		584	-						-	584
1.2.0	<Phase 1 Task 2 name>	6	385	108		400		1,800		2,308	1,400						-	3,708
1.2.1	<Subtask 1.2.1 name>	3	656	48		320		1,600		1,968	600						-	2,568
1.2.2	<Subtask 1.2.2 name>	3	113	60		80		200		340	800						-	1,140
:	:	:	:	:		:		:		:	:						:	:
		Phase 1 Total Hours		348		1,080		1,824		3,252	1,400						200	4,652
Phase 1 Costs *First column is prime, second is*								Travel		$ 44,000	$ 12,000						$ 2,000	$ 58,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ 8,000	$ -						$ -	$ 8,000
2.1.0	<Phase 2 Task 1 name>	8	100	176		560		64		800	100						100	1,000
2.1.1	<Subtask 2.1.1 name>	7	51	96		240		24		360	100						100	560
2.1.2	<Subtask 2.1.2 name>	4	110	80		320		40		440	-						-	440
2.2.0	<Phase 2 Task 2 name>	6	417	180		520		1,800		2,500	1,240						-	3,740
2.2.1	<Subtask 2.2.1 name>	4	435	140		400		1,200		1,740	400						-	2,140
2.2.2	<Subtask 2.2.2 name>	4	190	40		120		600		760	840						-	1,600
:	:	:	:	:		:		:		:	:						:	:
		Phase 2 Total Hours		356		1,080		1,864		3,300	1,340						100	4,640
Phase 2 Costs *First column is prime, second is*								Travel		$ 47,000	$ 12,000						$ 2,000	$ 61,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ 4,000	$ -						$ -	$ 4,000
3.1.0	<Phase 3 Task 1 name>	9	71	120		400		120		640	100						100	840
3.1.1	<Subtask 3.1.1 name>	3	93	40		200		40		280	100						100	480
3.1.2	<Subtask 3.1.2 name>	6	60	80		200		80		360	-						-	360
3.2.0	<Phase 3 Task 2 name>	6	460	160		800		1,800		2,760	1,200						-	3,960
3.2.1	<Subtask 3.2.1 name>	4	370	80		400		1,000		1,480	600						-	2,080
3.2.2	<Subtask 3.2.2 name>	3	427	80		400		800		1,280	600						-	1,880
:	:	:	:	:		:		:		:	:						:	:
		Phase 3 Total Hours		280		1,200		1,920		3,400	1,300						100	4,800
Phase 3 Costs *First column is prime, second is*								Travel		$ 48,000	$ 12,000						$ 2,000	$ 62,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ -	$ -						$ -	$ -
		Project Total Hours		984		3,360		5,608		9,952	4,040						400	14,092
Total Project Costs *First column is prime, second is*								Travel		$ 139,000	$ 36,000						$ 6,000	$ 181,000
total subcontractor, third is total consultant, fourth is total								Materials & Equipment		$ 12,000	$ -						$ -	$ 12,000

Figure 4: Example level-of-effort summary table. Numbers illustrate roll-ups and subtotals. The SubC column captures all subcontractor hours and the Conslt column captures all consultant hours. The Skill set(s) columns should indicate an area of expertise (e.g., engineer, software developer, data scientist, subject matter expert).

d. Summary Slide

The submission of a PowerPoint slide summarizing the proposed effort is mandatory. A template PowerPoint slide will be provided on the System for Award Management, Contract Opportunities website, as well as on the Grants.gov website, as an attachment. Submit the PowerPoint file (do not convert PowerPoint file to pdf format) in addition to Volume 1 and Volume 2 of your full proposal. This summary slide does not count towards the total page count.

2. Proprietary and Classified 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. 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.

a. Proprietary Information

Proposers are responsible for clearly identifying proprietary information. Submissions containing proprietary information must have the cover page and each page containing such information clearly marked.

b. Classified Information

Classified submissions (classified technical proposals or classified appendices to unclassified proposals) will not be accepted under this solicitation.

C. Submission Date and Time

Proposers are warned that submission deadlines as outlined herein are strictly enforced. Note: some proposal requirements may take from 1 business day to 1 month to complete. See the proposal checklist in Section VIII.C for further information.

When utilizing the DARPA BAA Submission Website, as described below in Section IV.E.1 below, a control number will be provided at the conclusion of the submission process. This control number should be used in all further correspondence regarding your abstract/proposal submission.

For proposal submissions requesting cooperative agreements, Section IV.E.1.c, you must request your control number via email at Ops-5G@darpa.mil. Please note that the control number will not be issued until after the proposal due date and time.

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

1. Proposals

The proposal package -- full proposal (Volume 1 and 2, LOE Spreadsheet and Summary PowerPoint Slide) and, as applicable, proprietary subcontractor cost proposals or classified appendices to unclassified proposals -- must be submitted per the instructions outlined herein and received by DARPA no later than **March 17, 2020 at 12:00 noon (ET)**. Proposal submissions received after this date and time will not be reviewed.

D. Funding Restrictions

Not applicable.

E. Other Submission Requirements

1. Unclassified Submission Instructions

Proposers must submit all parts of their submission package using the same method; submissions cannot be sent in part by one method and in part by another method nor should duplicate submissions be sent by multiple methods. Emailed submissions of abstracts or full

proposals will not be accepted.

a. Proposals Requesting a Procurement Contract or Other Transaction

DARPA/I2O will employ an electronic upload submission system (https://baa.darpa.mil/) for UNCLASSIFIED proposals requesting award of a procurement contract or Other Transaction under this solicitation.

First time users of the DARPA BAA Submission Website must complete a two-step account creation process at https://baa.darpa.mil/. The first step consists of registering for an Extranet account by going to the above URL and selecting the "Account Request" link on the right side of the page, using the Chrome browser. Upon completion of the online form, proposers will receive two separate emails; one will contain a user name and the second will provide a temporary password. Once both emails have been received, proposers must go back to the submission website and log in using that user name and password. After accessing the Extranet, proposers must create a user account for the DARPA BAA Submission Website by selecting the "Register Your Organization" link at the top of the page. The DARPA BAA Submission Website will display a list of solicitations open for submissions. Once a proposer's user account is created, they may view instructions on uploading their proposal.

Proposers who already have an account on the DARPA BAA Submission Website may simply log in at https://baa.darpa.mil/, select this solicitation from the list of open DARPA solicitations and proceed with their proposal submission. Note: Proposers who have created a DARPA BAA Submission Website account to submit to another DARPA Technical Office's solicitations do not need to create a new account to submit to this solicitation.

All submissions submitted electronically through DARPA's BAA website must be uploaded as zip files (.zip or .zipx extension). The final zip file should contain only the files requested herein and must not exceed 50 MB in size. Only one zip file will be accepted per submission. Note: Submissions not uploaded as zip files will be rejected by DARPA.

Please note that all submissions MUST be finalized, meaning that no further editing will be possible, when submitting through the DARPA BAA Submission Website in order for DARPA to be able to review your submission. If a submission is not finalized, the submission will not be deemed acceptable and will not be reviewed.

Website technical support may be reached at Action@darpa.mil and is typically available during regular business hours (9:00 AM – 5:00 PM ET, Monday-Friday). Questions regarding submission contents, format, deadlines, etc. should be emailed to OPS-5G@darpa.mil.

Since proposers may encounter heavy traffic on the web server, it is highly recommended that proposers not wait until the day proposals are due to request an account and/or upload the submission. Full proposals should not be submitted via Email. Any full proposals submitted by Email will not be accepted or evaluated.

b. Proposals Requesting a Cooperative Agreement

Proposers requesting cooperative agreements must submit proposals through one of the following methods: (1) electronic upload per the instructions at https://www.grants.gov/applicants/apply-for-grants.html; or (2) hard-copy mailed directly to DARPA. If proposers intend to use Grants.gov as their means of submission, then they must submit their entire proposal through Grants.gov; applications cannot be submitted in part to Grants.gov and in part as a hard-copy. Proposers using Grants.gov do not submit hard-copy proposals in addition to the Grants.gov electronic submission.

Submissions: Proposers must submit the three forms listed below.

Form 1: SF 424 Research and Related (R&R) Application for Federal Assistance, available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_SF424_2_0-V2.0.pdf. *This form must be completed and submitted.*

To evaluate compliance with Title IX of the Education Amendments of 1972 (20 U.S.C. § 1681 et.seq.), the Department of Defense (DoD) is collecting certain demographic and career information to be able to assess the success rates of women who are proposed for key roles in applications in science, technology, engineering or mathematics disciplines. In addition, the National Defense Authorization Act (NDAA) for FY 2019, Section 1286, directs the Secretary of Defense to protect intellectual property, controlled information, key personnel, and information about critical technologies relevant to national security and limit undue influence, including foreign talent programs by countries that desire to exploit United States' technology within the DoD research, science and technology, and innovation enterprise. This requirement is necessary for all research and research-related educational activities. The DoD is using the two forms below to collect the necessary information to satisfy these requirements. Detailed instructions for each form are available on Grants.gov.

The Research and Related Senior/Key Person Profile (Expanded) form will be used to collect the following information for all senior/key personnel, including Project Director/Principal Investigator and Co-Project Director/Co-Principal Investigator, whether or not the individuals' efforts under the project are funded by the DoD:

- Degree Type and Degree Year.
- Current and Pending Support, including:
    - A list of all current projects the individual is working on, in addition to any future support the individual has applied to receive, regardless of the source.
    - Title and objectives of the other research projects.
    - The percentage per year to be devoted to the other projects.
    - The total amount of support the individual is receiving in connection to each of the other research projects or will receive if other proposals are awarded.
    - Name and address of the agencies and/or other parties supporting the other research projects
    - Period of performance for the other research projects.

Additional senior/key persons can be added by selecting the "Next Person" button at the bottom of the form. Note that, although applications without this information completed may

pass Grants.gov edit checks, if DARPA receives an application without the required information, DARPA may determine that the application is incomplete and may cause your submission to be rejected and eliminated from further review and consideration under the BAA. DARPA reserves the right to request further details from the applicant before making a final determination on funding the effort.

Form 2: Research and Related Senior/Key Person Profile (Expanded), available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_KeyPersonExpanded_2_0-V2.0.pdf. *This form must be completed and submitted.*

Form 3: Research and Related Personal Data, available on the Grants.gov website at https://apply07.grants.gov/apply/forms/sample/RR_PersonalData_1_2-V1.2.pdf. *Each applicant must complete the name field of this form, however, provision of the demographic information is voluntary. Regardless of whether the demographic fields are completed or not, this form must be submitted with at least the applicant's name completed.*

Grants.gov requires proposers to complete a one-time registration process before a proposal can be electronically submitted. If proposers have not previously registered, this process can take between three business days and four weeks if all steps are not completed in a timely manner. See the Grants.gov user guides and checklists at https://www.grants.gov/web/grants/applicants.html for further information.

Once Grants.gov has received an uploaded proposal submission, Grants.gov will send two email messages to notify proposers that: (1) their submission has been received by Grants.gov; and (2) the submission has been either validated or rejected by the system. It may take up to two business days to receive these emails. If the proposal is rejected by Grants.gov, it must be corrected and re-submitted before DARPA can retrieve it (assuming the solicitation has not expired). If the proposal is validated, then the proposer has successfully submitted their proposal and Grants.gov will notify DARPA. Once the proposal is retrieved by DARPA, Grants.gov will send a third email to notify the proposer. If requested by the proposer, a control number for the cooperative agreement submission can be provided following the due date and time for the proposals. This control number should be used in all further correspondence regarding this submission.

To avoid missing deadlines, proposers should submit their proposals to Grants.gov in advance of the proposal due date, with sufficient time to complete the registration and submission processes, receive email notifications and correct errors, as applicable.

For more information on submitting proposals to Grants.gov, visit the Grants.gov submissions page at: http://www.grants.gov/web/grants/applicants/apply-for-grants.html.

Proposers electing to submit cooperative agreement proposals as hard copies must complete the SF 424 R&R form (Application for Federal Assistance, Research and Related) available on the Grants.gov website http://apply07.grants.gov/apply/forms/sample/RR_SF424_2_0-V2.0.pdf.

Proposers choosing to mail hard copy proposals to DARPA must include one paper copy and one electronic copy (e.g., CD/DVD) of the full proposal package.

Technical support for the Grants.gov website may be reached at 1-800-518-4726 and support@grants.gov. Questions regarding submission contents, format, deadlines, etc. should be emailed to OPS-5G@darpa.mil.

V. Application Review Information

A. Evaluation Criteria

Proposals will be evaluated 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 innovative, feasible, achievable, and complete.

  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.

  Proposer should also take note to the information provided in Section I, as DARPA will also look at how a proposer addresses the technical challenges relevant to each TA, as well as view how key personnel will work on those challenges.

- *Potential Contribution and Relevance to the DARPA Mission:*

  The potential contributions of the proposed effort are relevant to the national technology base. Specifically, DARPA's mission is to make pivotal early technology investments that create or prevent strategic surprise for U.S. National Security.
  This includes considering the extent to which any proposed intellectual property restrictions will potentially impact the Government's ability to transition the technology .

- *Cost Realism:*

  The proposed costs are realistic for the technical and management approach and accurately reflect the technical goals and objectives of the solicitation. The proposed costs are consistent with the proposer's Statement of Work and reflect a sufficient understanding of the costs and level of effort needed to successfully accomplish the proposed technical approach. The costs for the prime proposer and proposed subawardees are substantiated by the details provided in the proposal (e.g., the type and number of labor hours proposed per task, the types and quantities of materials, equipment and fabrication costs, travel and any other applicable costs and the basis for the estimates).

B. Review and Selection Process

The review process identifies proposals that meet the evaluation criteria described above and are, therefore, selectable for negotiation of awards by the Government. DARPA policy is to ensure

impartial, equitable, comprehensive proposal evaluations and to select proposals that meet DARPA technical, policy, and programmatic goals. If necessary, panels of experts in the appropriate areas will be convened. As described in Section IV, proposals must be deemed conforming to the solicitation to receive a full technical review against the evaluation criteria; proposals deemed non-conforming will be removed from consideration.

DARPA will conduct a scientific/technical review of each conforming proposal. Conforming proposals comply with all requirements detailed in this BAA; proposals that fail to do so may be deemed non-conforming and may be removed from consideration. Proposals will not be evaluated against each other since they are not submitted in accordance with a common work statement. DARPA's intent is to review proposals as soon as possible after they arrive; however, proposals may be reviewed periodically for administrative reasons.

Selections may be made at any time during the period of solicitation. Pursuant to FAR 35.016, the primary basis for selecting proposals for award negotiation shall be technical, importance to agency programs, and fund availability. Proposals that are determined selectable will not necessarily receive awards.

For evaluation purposes, a proposal is defined to be the document and supporting materials as described in Section IV.B. 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 the appropriate non-disclosure requirements. No submissions will be returned.

VI. Award Administration Information

A. Selection Notices

After proposal evaluations are complete, proposers will be notified as to whether their proposal was selected for award negotiation as a result of 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 for award negotiation, the Government will initiate those negotiations following the notification.

B. Administrative and National Policy Requirements

1. Intellectual Property

Proposers should note that the Government does not own the intellectual property of technical data/computer software developed under Government contracts; it acquires the right to use the technical data/computer software. Regardless of the scope of the Government's rights, performers may freely use their same data/software for their own commercial purposes (unless restricted by U.S. export control laws or security classification). Therefore, technical data and computer software developed under this solicitation will remain the property of the performers, though DARPA desires to have a minimum of Government Purpose Rights (GPR) to noncommercial technical data/computer software developed through DARPA sponsorship.

The program will emphasize creating and leveraging open source technology and architecture. Intellectual property rights asserted by proposers are strongly encouraged to be aligned with open source/open architecture regimes.

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. Intellectual Property Representations

All proposers must provide a good faith representation of either ownership or possession of appropriate licensing rights to all other IP to be used for the proposed project. Proposers must 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 IP in the conduct of the proposed research. If proposers desire to use proprietary software or technical data or both as the basis of their proposed approach, in whole or in part, they should: (1) clearly identify in Appendix A such software/data and its proposed particular use(s); (2) explain how the Government will be able to reach its program goals (including transition) within the proprietary model offered; and (3) provide possible nonproprietary alternatives in any area that might present transition difficulties or increased risk or cost to the Government under the proposed proprietary solution.

b. Patents

All 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. Procurement Contracts

- **Noncommercial Items (Technical Data and Computer Software):** Proposers requesting a procurement contract must list all noncommercial technical data and computer software that it plans to generate, develop, and/or deliver, in which the Government will acquire less than unlimited rights and to assert specific restrictions on those deliverables. In the event a proposer does 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, 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, 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 solicitation. A template for complying with this request is provided in Section IV.B.2.a.xi.(5).

- **Commercial Items (Technical Data and Computer Software):** Proposers requesting a procurement contract must list all commercial technical data and commercial computer software that may be included in any 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. In the event a proposer does 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 solicitation. A template for complying with this request is provided in Section IV.B.2.a.xi.(5).

d. Other Types of Awards

Proposers responding to this solicitation requesting an award instrument other than a procurement contract shall follow the applicable rules and regulations governing those award instruments, but in all cases should appropriately identify any potential restrictions on the Government's use of any intellectual property contemplated under those award instruments in question. This includes both noncommercial items and commercial items. The Government may use the list as part of the evaluation process to assess 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 solicitation. A template for complying with this request is provided in Section IV.B.2.a.xi.(5).

2. Human Subjects Research (HSR)/Animal Use

Proposers that anticipate involving human subjects or animals in the proposed research must comply with the approval procedures detailed at http://www.darpa.mil/work-with-us/additional-baa, to include providing the information specified therein as required for proposal submission.

3. 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.

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

All proposers must be registered in SAM unless exempt per FAR 4.1102. FAR 52.204-7, "System for Award Management" and FAR 52.204-13, "System for Award Management Maintenance" are incorporated into this BAA. See http://www.darpa.mil/work-with-us/additional-baa for further information.

International entities can register in SAM by following the instructions in this link: https://www.fsd.gov/fsd-gov/answer.do?sysparm_kbid=dbf8053adb119344d71272131f961946&sysparm_search=KB0013221.

Note that new registrations can take an average of 7-10 business days to process in SAM. SAM registration requires the following information:

- DUNS number
- TIN
- CAGE Code. If a proposer does not already have a CAGE code, one will be assigned during SAM registration.

- Electronic Funds Transfer information (e.g., proposer's bank account number, routing number, and bank phone or fax number).

C. Reporting

1. Technical and Financial Reports

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

2. Representations and Certifications

In accordance with FAR 4.1102 and 4.1201, proposers requesting a procurement contract must complete electronic annual representations and certifications at https://www.sam.gov/. In addition, resultant procurement contracts will require supplementary DARPA-specific representations and certifications. See http://www.darpa.mil/work-with-us/additional-baa for further information.

3. Wide Area Work Flow (WAWF)

Unless using another means of invoicing, performers will be required to submit invoices for payment directly at https://wawf.eb.mil. If applicable, WAWF registration is required prior to any award under this solicitation.

4. Terms and Conditions

For terms and conditions specific to grants and/or cooperative agreements, see the DoD General Research Terms and Conditions (latest version) at http://www.onr.navy.mil/Contracts-Grants/submit-proposal/grants-proposal/grants-terms-conditions and the supplemental DARPA-specific terms and conditions at http://www.darpa.mil/work-with-us/contract-management#GrantsCooperativeAgreements.

5. FAR and DFARS Clauses

Solicitation clauses in the FAR and DFARS relevant to procurement contracts and FAR and DFARS clauses that may be included in any resultant procurement contracts are incorporated herein and can be found at www.darpa.mil/work-with-us/additional-baa.

See also Section II.C regarding the disclosure of information and compliance with safeguarding covered defense information controls (for FAR-based procurement contracts only).

6. i-Edison

Award documents 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.

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

Further information on Controlled Unclassified Information on Non-DoD Information Systems is incorporated herein can be found at www.darpa.mil/work-with-us/additional-baa.

VII. Agency Contacts

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

- **Technical POC:** Jonathan Smith, Program Manager, DARPA/I2O

- **Email:** OPS-5G@darpa.mil

- **Mailing address**:
  DARPA/I2O
  ATTN: HR001120S0026
  675 North Randolph Street
  Arlington, VA 22203-2114

- **I2O Solicitation Website:** http://www.darpa.mil/work-with-us/opportunities

VIII. Other Information

A. Frequently Asked Questions (FAQs)

Administrative, technical, and contractual questions should be sent via email to OPS-5G@darpa.mil. All questions must be in English and must include the name, email address, and the telephone number of a point of contact.

DARPA will attempt to answer questions in a timely manner; however, questions submitted within 7 days of closing may not be answered. If applicable, DARPA will post FAQs to http://www.darpa.mil/work-with-us/opportunities

B. Proposers Day

The Ops 5G Proposers Day was held on January 7, 2020, in Arlington, VA. The special notice regarding the Ops 5G Proposers Day, DARPA-SN-20-11, can be found at https://beta.sam.gov/opp/03c00d5d3213475a990d993290f8ee45/view

For further information regarding the Ops 5G Proposers Day, including slides from the event, please see http://www.darpa.mil/work-with-us/opportunities under HR001120S0026.

C. Submission Checklist

The following items apply prior to proposal submission. Note: some items may take up to 1 month to complete.

✓	Item	BAA Section	Applicability	Comment
	Obtain DUNS number	IV.B.2.a.i	Required of all proposers	The DUNS Number is the Federal Government's contractor identification code for all procurement-related activities. See http://fedgov.dnb.com/webform/index.jsp to request a DUNS number. Note: requests may take at least one business day.
	Obtain Taxpayer Identification Number (TIN)	IV.B.2.a.i	Required of all proposers	A TIN is used by the Internal Revenue Service in the administration of tax laws. See https://www.irs.gov/forms-pubs/about-form-w-9 for information on requesting a TIN. Note: requests may take from 1 business day to 1 month depending on the method (online, fax, mail).
	Register in the System for Award Management (SAM)	VI.B.4	Required of all proposers	The SAM combines Federal procurement systems and the Catalog of Federal Domestic Assistance into one system. See https://www.sam.gov for information and registration. Note: new registrations can take an average of 7-10 business days. SAM registration requires the following information: -DUNS number -TIN -CAGE Code. A CAGE Code identifies companies doing or wishing to do business with the Federal Government. If a proposer does not already have a CAGE code, one will be assigned during SAM registration. -Electronic Funds Transfer information (e.g., proposer's bank account number, routing number, and bank phone or fax number).

	Ensure eligibility of all team members	III	Required of all proposers	Verify eligibility, as applicable, for in accordance with requirements outlined in Section 3.
	Register at Grants.gov	IV.E.1.c	Required for proposers requesting grants or cooperative agreements	Grants.gov requires proposers to complete a one-time registration process before a proposal can be electronically submitted. If proposers have not previously registered, this process can take between three business days and four weeks if all steps are not completed in a timely manner. See the Grants.gov user guides and checklists at https://www.grants.gov/web/grants/applicants.html for further information.

The following items apply as part of the submission package:

✓	Item	BAA Section	Applicability	Comment
	Volume 1 (Technical and Management Proposal)	IV.B.2	Required of all proposers	Conform to stated page limits and formatting requirements. Include all requested information.
	Appendix A	IV.B.2.a.xi	Required of all proposers	-Team member identification - Government/FFRDC team member proof of eligibility - Organizational conflict of interest affirmations - Intellectual property assertions - Human subjects research - Animal use - Unpaid delinquent tax liability/felony conviction representations -CASB disclosure, if applicable
	Appendix B	IV.B.2.a.xii	Optional of all proposers	- Appendix B does not count against the page limit - A brief bibliography to relevant papers, reports, or resumes - Do not include technical papers - The materials in Appendix B will not be evaluated as part of the proposal review
	Volume 2 (Cost Proposal)	IV.B.2.b	Required of all proposers	- Cover Sheet - Cost summary - Detailed cost information including justifications for direct labor, indirect costs/rates, materials/equipment, subcontractors/consultants, travel, ODCs - Cost spreadsheet file (.xls or equivalent format) - If applicable, list of milestones for OTs - Subcontractor plan, if applicable Subcontractor cost proposals - Itemized list of material and equipment items to be purchased with vendor quotes or engineering estimates for material and equipment more than $50,000 - Travel purpose, departure/arrival destinations, and sample airfare
	Level of Effort Summary by Task Excel spreadsheet	IV.B.2.c	Required of all proposers	A template LoE Excel file will be provided on the Beta.Sam.gov website as an attachment. Submit the LoE Excel file (do not convert Excel file to pdf format).
	PowerPoint Summary Slide	IV.B.2.d	Required of all proposers	A template PowerPoint slide will be provided on the Beta.Sam.gov website as an attachment. Submit the PowerPoint file (do not convert PowerPoint file to pdf format).

D. Associate Contractor Agreement (ACA)

This same or similar language will be included in contract awards against HR001120S0026. Awards other than FAR based contracts will contain similar agreement language:

(a) It is recognized that success of the OPS-5G research effort depends in part upon the open exchange of information between the various Associate Contractors involved in the effort. This language is intended to insure that there will be appropriate coordination and integration of work by the Associate Contractors to achieve complete compatibility and to prevent unnecessary duplication of effort. By executing this contract, the Contractor assumes the responsibilities of an Associate Contractor. For the purpose of this ACA, the term Contractor includes subsidiaries, affiliates, and organizations under the control of the contractor (e.g. subcontractors).

(b) Work under this contract may involve access to proprietary or confidential data from an Associate Contractor. To the extent that such data is received by the Contractor from any Associate Contractor for the performance of this contract, the Contractor hereby agrees that any proprietary information received shall remain the property of the Associate Contractor and shall be used solely for the purpose of the OPS-5G research effort. Only that information which is received from another contractor in writing and which is clearly identified as proprietary or confidential shall be protected in accordance with this provision. The obligation to retain such information in confidence will be satisfied if the Contractor receiving such information utilizes the same controls as it employs to avoid disclosure, publication, or dissemination of its own proprietary information. The receiving Contractor agrees to hold such information in confidence as provided herein so long as such information is of a proprietary/confidential or limited rights nature.

(c) The Contractor hereby agrees to closely cooperate as an Associate Contractor with the other Associate Contractors on this research effort. This involves as a minimum:

(1) maintenance of a close liaison and working relationship;

(2) maintenance of a free and open information network with all Government-identified associate Contractors;

(3) delineation of detailed interface responsibilities;

(4) entering into a written agreement with the other Associate Contractors setting forth the substance and procedures relating to the foregoing, and promptly providing the Agreements Officer/Procuring Contracting Officer with a copy of same; and,

(5) receipt of proprietary information from the Associate Contractor and transmittal of Contractor proprietary information to the Associate Contractors subject to any applicable proprietary information exchange agreements between associate contractors when, in either case, those actions are necessary for the performance of either.

(d) In the event that the Contractor and the Associate Contractor are unable to agree upon any such interface matter of substance, or if the technical data identified is not provided as scheduled, the Contractor shall promptly notify the DARPA Ops 5G Program Manager. The Government will determine the appropriate corrective action and will issue guidance to the affected Contractor.

(e) The Contractor agrees to insert in all subcontracts hereunder which require access to proprietary information belonging to the Associate Contractor, a provision which shall conform substantially to the language of this ACA, including this paragraph (e).

(f) Associate Contractors for the Ops 5G research effort include:

Contractor	Technical Area

(End of Clause)

For information concerning agency level protests see http://www.darpa.mil/work-with-us/additional-baa#NPRPAC.

---

[i] "Technical Specification: System Architecture for the 5G System (3GPP TS 23.501 version 15.2.0 Release 15)" ETSI, 650 Route de Lucioles, F-0692 Sophia Antipolis, Cedex - FRANCE, June 2018.
[ii] "OpenFlow: Enabling Innovation in Campus Networks", N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker and J. Turner, ACM Computer Communications Review, 2008.
[iii] "P4: Programming Protocol-Independent Packet Processors", P. Bosshart, D. Daly, M. Izzard, N. McKeown, J. Rexford, D. Talayco, A. Vahdat, G. Varghese, D. Walker, ACM Computer Communications Review, July 2014.
[iv] "Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system (Release 15)", *Technical Specification 3GPP TS 33.501 V15.5.0 (2019-06),* June 2019.
[v] "The Evolution of Security in 5G: A 'Slice' of Mobile Threats", *5G Americas White Paper*, July 2019.
[vi] "The Athens Affair: How Some Extremely Smart Hackers Pulled Off the Most Audacious Cell-network Break-In Ever", Vassilis Prevelakis and Diomidis Spinellis, *IEEE Spectrum*, 2007.
[vii] "The Cathedral and the Bazaar", Eric S. Raymond, 1997.
[viii] "Experiences Enhancing Security of Open Source Software in the POSSE Project", J. M. Smith, M. B. Greenwald, S. Ioannidis, A. D. Keromytis, B. Laurie, D. Maughan, D. Rahn and J. Wright, In Free/Open Source Software Development, Stefan Koch (editor), pp. 240 - 255. Idea Group Publishing, July, 2004.
[ix] "Portability of C Programs and the UNIX System", S. C. Johnson and D. M. Ritchie, *The Bell System Technical Journal*, **57**(6), Part 2, July/August 1978, pp. 2021-2048.
[x] "Active networking: One view of the past, present, and future", J. M. Smith and S. M. Nettles, *IEEE Trans. Syst., Man, and Cybernetics, Part C: Applications and Reviews*, **34**(1), February 2004, pages 4-18.
[xi] "Build Security Into Your Network's DNA: The Zero Trust Network Architecture", J. Kindervag, Forrester, Nov. 2010.
[xii] "Verifying and Enforcing Network Paths with Icing", J. Naous, M. Walfish, A. Nicolosi, D. Mazieres, M. Miller, A. Seehra, in *Proc. CoNEXT 2011*.
[xiii] "Toward Automated International Law Compliance Monitoring (TAILCM): Final Technical Report", LEIDOS, Inc., *Air Force Research Laboratory Technical Report AFRL-RI-RS-TR-2014-206*, July 2014.
[xiv] "The Universal Parser Architecture for Knowledge Based Machine Translation", Masaru Tomita, Jaime G. Carbonell, Institute for Software Research, School of Computer Science, CMU, 1987.
[xv] "ARSENAL: Automated Requirements Specification from Natural Language", S. Ghosh, D. Elenius, W. Li, P. Lincoln, N. Shankar and W. Steiner, in *Proc. NASA Formal Methods Symposium*, 2016.
[xvi] "Recoverability of communications protocols – implications of a theoretical study", P. Merlin and D. J. Farber, in *IEEE Transactions on Computers*, COM-24:1036-1043, Sept. 1976.
[xvii] "CESEL: Securing a Mote for 20 Years", K. Kiningham, M. Horowitz, P. Levis and D. Boneh, Proc. 2016 International Conf. on Embedded Wireless Systems and Networks, pp. 307-312.
[xviii] "Trusted Platform Module (TPM) 2.0: A Brief Introduction", Trusted Computing Group, 2015.
[xix] "Titan silicon root of trust for Google Cloud", S. Johnson and D. Rizzo, Secure Enclaves Workshop, 8/29/18.
[xx] "The international telecommunication charge card", ITU-T E.118, 05/2006.
[xxi] "GSMA Explores Software-Based Replacement for mobile SIM Cards". Diana ben-Aaron, Bloomberg News, Nov. 18, 2010.

[xxii] "A Secure and Reliable Bootstrap Architecture", W. A. Arbaugh, D. J. Farber and J. M. Smith, in *Proceedings, IEEE Symposium on Security and Privacy*, Oakland, CA May 4-7, 1997.
[xxiii] "JEDI: Many-to-Many End-to-End Encryption and Key Delegation for IoT", S. Kumar, Y. Hu, M. P. Andersen, R. A. Popa and D.E. Culler, in *Proc. USENIX Security*, 2019.
[xxiv] "Zero Trust Networks", D. Barth and E. Gilman, O'Reilly, 2017.
[xxv] "The Protection of Information in Computer Systems", Proc. IEE, 1975, pp. 1278-1308.
[xxvi] "Least Privilege and More", F.B. Schneider, in "Computing Systems: Theory, Technology and Applications (A Tribute to Roger Needham)", Springer, 2004.
[xxvii] "WAVE: A Decentralized Authorization Framework with Transitive Delegation", M. P. Andersen, S. Kumar, M. AbdelBaky, G. Fierro, J. Kolb, H.-S. Kim, D. E. Culler and R. A. Popa, in *Proc. USENIX Security* 2019.
[xxviii] "The Evolution of Security in 5G: A 'Slice' of Mobile Threats", *5G Americas White Paper*, July 2019.
[xxix] "Hey you, get off my cloud: exploring information leakage in third-party compute clouds", T. Ristenpart, E. Tromer, H. Shacham and S. Savage, in *Proc. ACM CCS*, 2009.
[xxx] "Probabalistic Logics and the Synthesis of Reliable Organisms from Unreliable Components", J. von Neumann, in *Automata Studies*, ed. Claude Shannon, Princeton University Press, 1956.
[xxxi] "Verifying and Enforcing Network Paths with Icing", J. Naous, M. Walfish, A. Nicolosi, D. Mazieres, M. Miller, A. Seehra, in *Proc. CoNEXT 2011*.
[xxxii] "A brief overview of the NEBULA Future Internet Architecture", T. Anderson, K. Birman, R. Broberg, M. Caesar, D. Comer, C. Cotton, M. J. Freedman, A. Haeberlen, Z. G. Ives, A. Krishnamurthy, W. Lehr, B. T. Loo, D. Mazières, A. Nicolosi, J. M. Smith, I. Stoica, R. Van Renesse, M. Walfish, H. Weatherspoon and C. S. Yoo, in ACM Computer Communications Review, **44**(3), July 2014, pp. 81-86.
[xxxiii] "Proof Carrying Code", G. Necula, ACM Symposium on Principles of Programming Languages, 1997, pp. 106-119.
[xxxiv] "The Price of Safety in an Active Network", D. S. Alexander, P. B. Menage, A. D. Keromytis, W. A. Arbaugh, K. G. Anagnostakis and J. M. Smith, in *Journal of Communications and Networks*, KICS, 2001.
[xxxv] "Practical Programmable Packets", Jonathan T. Moore, Michael W. Hicks and Scott M. Nettles, in *Proc. IEEE Infocom*, 2002.
[xxxvi] "Implementing Pushback: Router-based Defenses Against Denial of Service", J. Ioannidis and S. Bellovin, in *Proc. NDSS*, 2002.
[xxxvii] "Understanding the Mirai Botnet", Manos Antonakakis, et al., in *Proc. USENIX Security*, August 2017.
[xxxviii] http://mininet.org/