

Broad Agency Announcement Solicitation 70RSAT19RB00000001
Project: Secure and Resilient Mobile Network Infrastructure (SRMNI)

1. Introduction

This BAA solicitation is a call issued against Department of Homeland Security (DHS), Science and Technology Directorate (S&T), 5-Year Broad Agency Announcement (BAA), HSHQDC-17-R-B0002 (current issue)¹. All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002 (current issue), apply to this solicitation unless otherwise noted herein.

This BAA Call is identified by its Procurement Instrument Identifier 70RSAT19RB00000001.

The DHS Study on Mobile Device Security² identified threats to, and security challenges in, mobile network infrastructure that could negatively impact the Government's use of mobile technologies. It also identified the need for government research and development (R&D) to address the risks. Targeted R&D could inform development and adoption of standards to improve security and resilience of critical mobile communications networks.

2. Project Description and Scope

As shown in Figure 1, mobile device and mobile network elements extend from the mobile device through the radio access and core networks to the Internet and into enterprise systems. S&T seeks innovative approaches to improve protection of the cellular mobile infrastructure against threats indicated with a star in the figure. These threats impact the following elements of the mobile network infrastructure:

- The air interface between the mobile device and the Radio Access Network (RAN)
- The RAN cellular tower/base station
- Virtualized elements of the RAN or the core network
- Signaling System 7 (SS7), Diameter, and other signaling protocols within the cellular core network
- Traffic sent from the core network to the internet or enterprise systems, across third party transport networks connecting RAN and core networks, and connectivity to Public Safety Answering Points (PSAPs).
- Security of enterprise systems and data accessed via mobile technologies

The S&T Mobile Security Research and Development ("Mobile Security R&D") program's security and resilience of mobile network infrastructure R&D projects seek innovative approaches and technologies to protect legacy, current, and 5G mobile network communications, services, and equipment against these threats. Pertinent discussion of the mobile network infrastructure, including current and legacy protocols, is below.

¹ <https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-17-R-B0002/listing.html>

² DHS S&T, "DHS Study on Mobile Device Security," DHS, Washington, 2017. [Online]. Available: <https://www.dhs.gov/publication/csd-mobile-device-security-study>. [Accessed 22 March 2019]

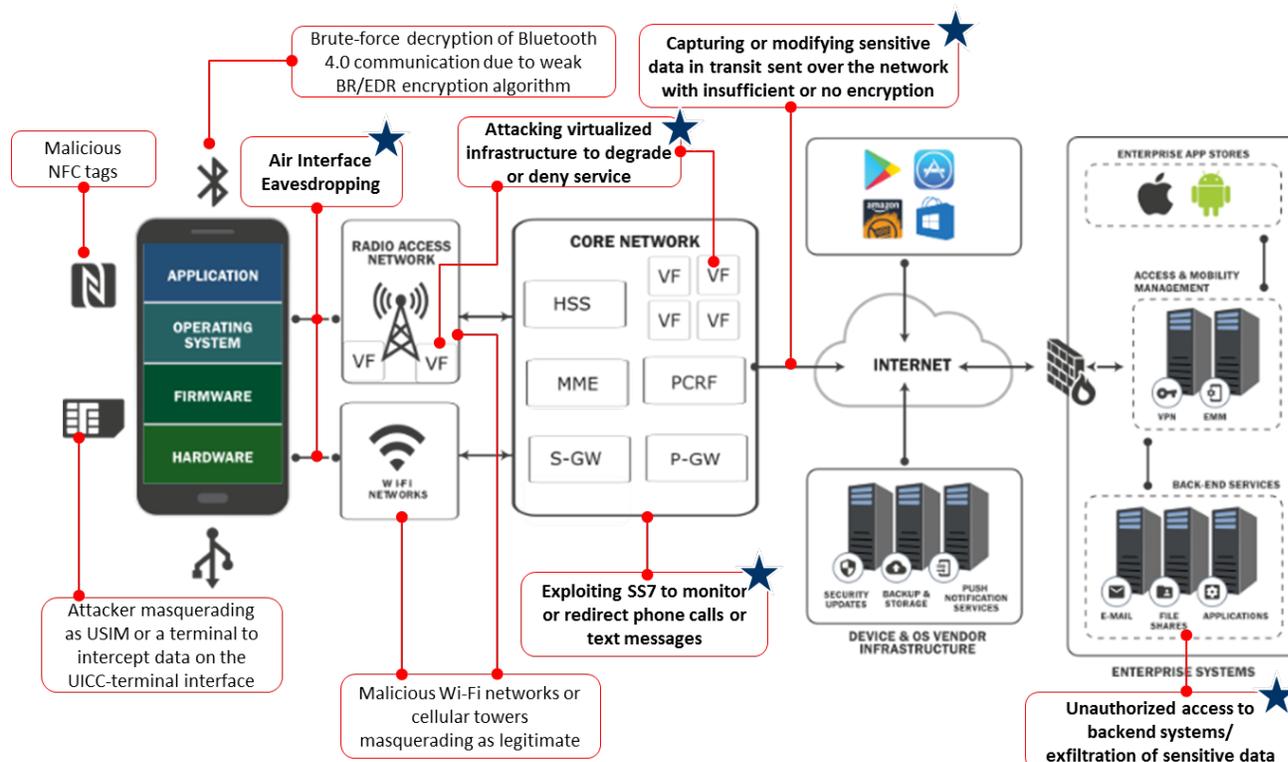


Figure 1. Threats to Mobile Network Infrastructure

2.1 Legacy (2G and 3G) Networks and Signaling Standards

SS7 is the global signaling standard and data exchange protocol used to connect the Public Switched Telephone Network (PSTN) and 2G/3G carriers worldwide. In 4G Long Term Evolution (LTE) core networks, the Diameter protocol replaces SS7, but interfaces with the SS7 network to provide interoperability through an Interworking Function (IWF). SS7 networks are a critical information-sharing element of the core network. Traditionally owned by Mobile Network Operators (MNOs) and global telephone companies, businesses and individuals can now rent access from domestic and international providers, whether for legitimate or malicious use. Built on a model of a relatively small number of trusted carriers, SS7 does not include authentication between networks. This design has been exploited by attackers to perform location tracking, intercept calls and Short Message Service (SMS) messages, deny service, and commit financial fraud³. Many services depend on SS7, including local number portability, SMS, toll-free and toll wireline services, call features such as call forwarding, calling party name/number display, and three-way calling. Although legacy cellular networks in the U.S. are being replaced by 4G LTE—estimated to cover over 99% of the population per the Federal Communications Commission’s (FCC) report⁴—worldwide, the 4G implementation rate is at

³ Wired.com, "Fixing the Cell Network Flaw That Lets Hackers Drain Bank Accounts," 9 May 2017. [Online]. Available: <https://www.wired.com/2017/05/fix-ss7-two-factor-authentication-bank-accounts/>. [Accessed 22 March 2019].

⁴ FCC, "Twentieth Mobile Wireless Competition Report," 7 September 2017. [Online]. Available: https://apps.fcc.gov/edocs_public/attachmatch/DOC-346595A1.pdf. [Accessed 22 March 2019].

43% and expected to reach 60% in 2023⁵, meaning that SS7 will be around for a long time.

The FCC's Communications Security Reliability and Interoperability Council (CSRIC)⁶ recommended that U.S. MNOs adopt SS7 security standards and best practices developed by the Third Generation Partnership Project (3GPP) and GSMA (Groupe Spécial Mobile (GSM) Association) to protect their networks and subscribers. However, challenges remain as there is limited understanding of what SS7 traffic can be filtered without breaking diverse market-driven services. Security challenges in SS7 may be propagated to 4G Diameter networks through the IWF; and Diameter may have its own set of Internet Protocol (IP) security challenges that require mitigation.⁷ Products are available that allow carriers to filter traffic, detect intrusions, and scan for vulnerabilities; but carriers are cautious in implementing the products as most SS7 traffic is legitimate.

Diameter was designed as an extensible protocol, which already incorporates more than 80 sub-protocols called "applications". Although there are no public reports of exploits against the protocol, there is a need to investigate security weaknesses in the base protocol and its applications and identify mitigations. For both signaling protocols, efforts are needed to improve understanding of what data fields and traffic can be filtered for sharing outside of trusted partners. Additionally, protections are implemented independently by each provider, making implementing and testing security controls complex.

2.2 Current (4G) Network

LTE is the 4G standards-based cellular technology, and it is being deployed by MNOs globally. It is also the recommended wireless technology for the 700 megahertz (MHz) public safety network (FirstNet) in the U.S. However, LTE technologies have known security challenges. Current LTE networks rely on packet switching, rather than the circuit switched networks used in earlier generations. The use of packet switching and the IP protocol may allow for new types of attacks not possible on previous generation networks.

Research is needed to address existing threats and develop vendor agnostic mitigation approaches and methods to protect the core and radio access network. Techniques and products to mitigate certain LTE security challenges exist; however, work is needed to design a family of integrated techniques to address these challenges.

2.3 Fifth Generation Network

5G is the evolution of 4G technologies. Work on this standard for the next generation mobile network was initiated to handle the ever-increasing demand for higher data rates, lower latency, and higher reliability that cannot be met by LTE alone. The three core use cases for 5G as

⁵ GSMA, "The Mobile Economy 2019." 25 February 2019. [Online]. Available:

<https://www.gsmainelligence.com/research/2019/02/the-mobile-economy-2019/731/> [Accessed 26 March 2019].

⁶ FCC Communications Security, Reliability, and Interoperability Council (CSRIC), "Working Group 10 Legacy Systems Risk Reductions Final Report," March 2017. [Online]. Available: <https://www.fcc.gov/files/csric5-wg10-finalreport031517pdf>. [Accessed 22 March 2019].

⁷ FCC, CSRIC, "Final Report – Recommendations to Mitigate Security Risks for Diameter Networks", Version 1.1, 14 March 2018. [Online]. Available: <https://www.fcc.gov/files/csric6wg3finalreport32018pdf>. [Accessed 26 March 2019]

outlined by 3GPP are Ultra-Reliable Low-Latency Communications (URLLC), Enhanced Mobile Broadband (eMBB), and Massive Machine Type Communications (mMTC). Each use case has a unique set of capabilities and risks (e.g., use of small or micro cells) that will meet different requirements within the government. Although 5G phase 1 standards have been completed in R-15 and 3GPP is working on the 5G phase 2 standards in R-16, there is still an opportunity for the government to influence the standards to provide specific security requirements needed by the government for R-16 and beyond.

In the LTE security architecture, it is difficult to implement government security policy on top of cellular networks. With the 5G network, a virtual network technique called network slicing can virtually slice a portion of RAN and core network resources. For government usage, network slicing may provide the functionality to comply with additional government security requirements, provide the government with a certain Quality of Service (QoS), or segregate government traffic. Network slicing allows multiple virtual networks to be created on a common physical infrastructure; the virtual networks are then customized to meet specific application, service, or customer needs. This technique may also slice layers of security stacks to dynamically meet government security requirements (e.g., confidentiality and integrity protections, authentication, and non-repudiation) and environments. Such 5G environments may be implemented as a network of networks with multiple RAN technologies (5G NR, LTE, Satellite, WiFi) connecting into a single core or different provider core networks making identification and authentication of a user or device more challenging. Such implementation also presents potential attack points at each network-to-network interface to the Internet, PSAPs, Land Mobile Radio (LMR) networks (via IWF), and intermediate transport networks, which will not be under the control/network slice purview of one provider end to end.

Current 4G cellular systems encrypt traffic from the User Equipment (UE) (i.e., mobile device) to the base station, but do not necessarily encrypt user traffic as it is backhauled through the 4G carrier's network. This potential lack of encryption leaves user data at risk of eavesdropping and user systems susceptible to man-in-the-middle attacks. This deficiency can be mitigated in 5G through development of techniques and approaches to encrypt traffic from the UE to the core network. A related need is for methods that enable interoperable, government-managed secure voice and video communications for federal government users at the FOUO level.

For 5G phase 1, the 4G core will still be used to support non-standalone configuration. However, in 5G phase 2, the new 5G core will be deployed. In the new 5G core, the Diameter protocol will be replaced with a common control protocol using Hyper Text Transfer Protocol (HTTP) 2.0 with Representational State Transfer (RESTful) application programming interfaces (API).

2.4 Enterprise Visibility of Mobile Network Traffic

Much of the protection for federal enterprise systems is provided at the enterprise network edge through firewalls and the Trusted Internet Connection (TIC) at the interface to the Internet. With mobile devices, instead of a multilayered approach that protects federal enterprise systems, mobile devices communicate directly with untrusted networks. Furthermore, in some cases, these devices can download untrusted applications which also communicate directly with the Internet. This approach makes it difficult to protect enterprise systems and data against unpatched devices or zero day attacks. As enterprises and commercial technologies enable more mobile access to

enterprise data and systems, it is imperative that more visibility and control be provided into the actions performed by mobile devices.

3. Technical Topic Areas (TTAs)

In this SRMNI BAA call, DHS is seeking the development of technologies to improve the security and resilience of the mobile network infrastructure, including 2G, 3G, LTE/4G, and emerging 5G technologies. TTA #1 focuses on 2G, 3G, and 4G network protections. TTA #2 focuses on building security in to 5G networks and leveraging 5G to demonstrate solutions that meet government security needs. Another focus of TTA #2 is end-to-end protection of network traffic, including a development of a standardized secure voice and video capability for unclassified government communications. Lastly, TTA #3 seeks innovative approaches to improve government visibility of network traffic from mobile devices to identify potential malware, attacks, or attempts to exfiltrate data from or through the device.

3.1 TTA #1: Threat Detection and Protection of Current and Legacy Protocols and Networks

TTA #1 seeks approaches to protect cell phone users from being tracked, having their calls and text messages monitored without user authorization, or hijacked due to inherent SS7/Diameter challenges. It also seeks vendor agnostic techniques to protect the core network.

3.1.1 Goal 1 – Data Filtering and Anomaly Detection to Improve SS7 Security

The first goal of this TTA is to develop and demonstrate technologies to monitor, detect, and respond to anomalous or potentially malicious use of SS7 networks. Technical approaches should address one or more of the following, but may propose other approaches to securing SS7 with a justification for doing so:

- Identify SS7 information that should be shared among trusted entities or anonymized for sharing with untrusted parties.
- Identify data elements that should be shared and when (e.g., only those mobile users who subscribe to international roaming should respond to international requests for user location).
- Identify data elements that could be anonymized to reduce data exposure; e.g., not providing international partners the exact location of a U.S. phone unless it is within 20 miles of the border.
- How to identify impossible situations that indicate malicious activity (e.g., a phone's location changing from the U.S. to Asia in less than 6 hours).
- How to distinguish between trusted and untrusted external requests.
- How to limit information that is exchanged with requesters from outside of the U.S.
- How to identify potential partners, performers and stakeholders for SS7 outsourced services through IP exchange (IPX).

3.1.2 Goal 2 – Threat Assessment and Mitigations for the Diameter IWF

The second goal of this TTA is to identify and eliminate weaknesses in the SS7/Diameter IWF to reduce the attack surface before vulnerabilities are discovered and exploited. Technical approaches should describe methods that would enable MNOs to clearly differentiate whether data requests received through the IWF are from untrusted or trusted external partners. Technical

approaches should consider how to identify risk factors that can be used to assess requester identity and filter malicious traffic. Technical approaches should also include providing capabilities to categorize the Diameter LTE interfaces (e.g., internal, 2G/3G, roaming partners, and PSTN) and developing recommendations for security requirements for each type of interface, to include recommendations for how to reduce sharing of private information based on the level of trust associated with an interface.

3.1.3 Goal 3 – Vendor Agnostic Protection Methods for the Core Network

The third goal of TTA #1 is to develop vendor agnostic protection methods for the LTE core network and validate them in a testbed environment. The proposed technical approaches need to describe the creation and demonstration of capabilities to discover the elements of the core LTE network and map them to a template according to 3GPP standards. Proposals must also describe how a test plan to assess deviations from the 3GPP standards would be developed, to include requirements needed for the testbed. During the discovery, the security protections present on the network, such as Virtual Private Network (VPN), firewalls and packet filtering, need to be identified and reported. Once the security protections are assessed and compared to government requirements and 3GPP standards, security gaps need to be identified and mitigated. The final effort for this TTA involves developing vendor-agnostic approaches to mitigate remaining security gaps and demonstrating the approaches in a testbed environment.

3.2 TTA #2: Fifth Generation (5G) Network Security

TTA #2 seeks the development of security capabilities that leverage 5G virtual functions/network slicing to define methods and approaches to achieve: a) flexible 5G security architecture tailored for government environments; b) government controlled security policy; c) end-to-end security for UE to the core; and d) secure voice implementation for federal government users. Technical approaches should indicate whether the approach supports 5G phase 1, 5G phase 2, or both, and whether the 3GPP standards will require changes to implement the approaches demonstrated. The security implications of moving to a new protocol and any need to support backwards compatibility with SS7 and Diameter may also be areas for research, if new protocols are part of the technical approach.

3.2.1 Goal 1 - Unified Family of 5G Security Techniques

The first goal of TTA #2 is the development of integrated 5G techniques to address LTE security challenges that are carried over to 5G networks and new threats introduced by 5G. The 4G threats that are carried over to 5G include distributed denial of service (DDoS) attacks, network configuration sniffing, and geolocation of mobile devices. The 5G unique threats include software exploitation of the virtualized RAN and core network and risks associated with software-defined networking for the core network. Technical approaches need to demonstrate an integrated set of techniques and approaches to address these threats. Proposals should also include approaches to mitigate threats and vulnerabilities of the anticipated high quantity of unprotected/exposed small cells in dense network areas such as cities and threats and attack surface presented by the sheer number of Internet of Things (IoT) devices that will be operating on 5G. Approaches should also examine how to address supply chain risks, which are not unique to 5G, but amplified by the variety of RAN technologies, devices, and networks that 5G will use.

3.2.2 Goal 2 – Security Architecture for Government Using Network Slicing

The second goal of TTA #2 is to define and demonstrate a flexible security architecture with network slicing capability that can be dynamically altered to meet regulated security requirements (e.g., confidentiality and integrity protections, protection of user identity and location, and authentication of sending and receiving entities). Technical approaches must also describe how the approach to meet government missions would be demonstrated, including any required capabilities for a testbed. The ability of a technical approach to adjust to on-demand changes to government requirements (e.g., security classifications) and environments (e.g., enterprise vs. tactical) will be considered reflective of flexibility.

3.2.3 Goal 3 – End-to-End Security from the Mobile Device to the Core

The third goal of TTA #3 is to implement end-to-end 5G encryption from the UE to a secure node within the core network or outside of the core network (e.g., government security enforcement point). Such methods will protect mobile users against eavesdropping and man-in-the-middle attacks. Technical approaches must also describe how the approach to meet government missions would be demonstrated, including required testbed capabilities. The security protection of the approaches will need to be demonstrated in a testbed environment, with the ability to change encryption policy (e.g., key size and encryption algorithm) based on government requirements.

3.2.4 Goal 4 – Interoperable Secure Voice for the Federal Government

The fourth goal of TTA #2 is to implement interoperable secure unclassified voice across Federal Government agencies. Technical approaches should describe the necessary components and standards that should be followed to deliver encrypted interoperable voice between mobile devices and between mobile devices and voice gateways for communications to landline networks. The technical approach must also identify the coder-decoders (CODECs) to be used, the encryption to be used, and Session Initiation Protocol (SIP) parameters that would be employed. The transition plan description must provide details for how government enterprises would manage and secure the proposed system. The proposed solution must utilize government approved encryption methods, define cellular QoS to be provided, and define expected audio quality as a function of packet loss. Proposing an optional pilot of the proposed solution is desired by DHS.

3.3 TTA #3: Mobile Network Traffic Visibility for the Enterprise

TTA #3 seeks to improve protection for mobile devices and enterprise backend systems in managed mobile networks by monitoring traffic from mobile devices. While adhering to all privacy laws and regulations, there are three goals for this TTA described in greater detail below. The first goal is to develop and implement a capability to identify suspicious network traffic patterns. The second goal is develop methods to direct mobile traffic into an enterprise controlled filtering system. Lastly, the third goal is to develop methods to categorize mobile traffic to support Goal 2.

3.3.1 Goal 1 – Track Mobile Traffic

The first goal of TTA #3 is to develop method(s) to enable enterprises to identify sources and destinations of mobile device traffic to enable identification of compromised devices. Technical approaches should provide a clear description of traffic flow monitoring to include, e.g., source

and destination IP address, IP protocol version and Transmission Control Protocol/User Datagram Protocol (TCP/UDP) port number. Additionally, the method should quantify the amount of traffic sent for each flow. This will enable identification of which networks and services mobile devices are communicating with and how much bandwidth each flow is consuming. Technical approaches should describe and demonstrate how the traffic flow data will be used to identify compromised devices.

3.3.2 Goal 2 – Enable Mobile Traffic Filtering

This goal seeks a second layer of protection of mobile device communications that is external to the mobile device. Historically, mobile systems have not been behind enterprise protection systems; proposers will need to identify methods to direct all (or part) of mobile traffic through enterprise controlled security protection systems to filter malware before it reaches the mobile devices. Ideally, the solution will enable redirection of all or part of mobile traffic to government security gateways.

3.3.3 Goal 3 – Categorization of Mobile Traffic

Supporting Goal 2, this goal seeks to document what types of iOS and Android traffic could be easily filtered and what types of traffic would likely remain unfiltered. For example, some encrypted traffic and secondary channels into mobile devices will be difficult to filter. Approaches and techniques should catalog the various categories of traffic communicating with mobile devices and demonstrate which commonly available filtering solutions would be able to filter each type of traffic.

4. Project Oversight and Monitoring

To keep pace with the mobile threat environment, the SRMNI project emphasizes frequent evaluations. Section 5 shows the project schedule and milestones, which includes progress meetings for DHS to be apprised of development toward project goals, and required Go/No-Go demonstrations on six (6) month intervals (excluding the Pilot Option). The optional Pilot Task for an additional six (6) months beyond the proposed technology development R&D work effort should focus on the integration and/or deployment of the completed solution into operation, as coordinated with DHS. The Pilot option would only be exercised after the successful development and identification of an interested DHS entity, Federal Government partner, or international partner within the Homeland Security Enterprise (HSE⁸). The partnering organization can be identified during the execution of the base effort. Finally, project management will be accomplished by having a kick-off meeting within one month following contract award. Key technical deliverables, pilot deliverables, and program status deliverables are listed below.

In addition, the intent of the Go/No-Go decision points on six (6) month intervals is to allow the Government to have flexibility to not only ensure that technical progress is being achieved, but also to adapt to trending mobile technologies; as such, award terminations may

⁸ DHS defines the homeland security enterprise as the federal, state, local, tribal, territorial, nongovernmental, and private-sector entities, as well as individuals, families, and communities, who share a common national interest in the safety and security of the United States and the American population (GAO, *Department of Homeland Security: Progress Made and Work Remaining after Nearly 10 Years in Operation*, [GAO-13-370T](#) (Washington, D.C.: Feb. 15, 2013)).

occur based on the Go/No-Go determinations.

4.1 Project Status Deliverables

The following project status deliverables are required throughout the period of performance:

DELIVERABLE	DUE DATE
Project Kickoff Briefing	Within fifteen (15) days of award
Presentation Materials from Project Meetings	Within five (5) days of presentation
Monthly Technical and Financial Status Reports	Starting on the fifteenth (15 th) day of the month, beginning in the calendar month after award, and the fifteenth (15 th) day of each month thereafter throughout the period of performance.
Program Reviews	3 and 5 months after award of the base period, and 4, 8 and 11 months after the exercise of each option thereafter. These may be either in-person or via phone or webex.

4.2 Key Technical Deliverables

The following key deliverables are required for each severable period of performance (note: for each successive year of performance, the version numbers will increase sequentially):

DELIVERABLES	DUE DATE
Monthly Technical and Financial Status Reports	Starting 45 days after award
Design Document, Version 1	45 days after award
Target Capabilities Definition Document, Version 1	45 days after award
Design Document, Version 2	5 months after award
Target Capabilities Definition Document, Version 2	5 months after award
Working Prototype, Version 1	5 months after award
Go/No-Go Demonstration Evaluation Plan	5 months after award
Go/No-Go Demonstration	5 months after award
Go/No-Go Demonstration Report	6 months after award
Go/No-Go Demonstration Evaluation Plan	10 months after award
Design Document, Version 3	11 months after award
Target Capabilities Definition Document, Version 3	11 months after award
Working Prototype, Version 2	11 months after award
Go/No-Go Demonstration	11 months after award
Go/No-Go Demonstration Report	12 months after award

4.3 Pilot Deliverables

The following key deliverables are required for all pilots, including the Pilot Option:

DELIVERABLES	DUE DATE
Pilot Demonstration Plan	3 months after the before Pilot Option is exercised
Pilot Demonstration Report	1 month after Pilot execution

4.4 Expected Award Funding Profile by TTA

Notwithstanding paragraph 2.2 of BAA HSHQDC-17-R-B0002, proposal types will not be used for this BAA Call.

The anticipated period of performance for any award is expected to be no more than four (4) years, inclusive of any options. The expected maximum total dollar value for any award made under TTAs 1 and 2 is \$2.75M, inclusive of any options. The expected maximum total dollar value for any award made under TTA 3 is \$2M, inclusive of any options. DHS gives higher consideration to proposals at, or within, the stated dollar values for a given TTA than to similarly-rated proposals that exceed the stated dollar value for a given TTA. In the event a proposal selected for award negotiations addresses more than one, or parts of more than one, TTA, the total amount of the predominant TTA the proposal addresses will be used.

5. Special Instructions/Notifications

5.1 Response Dates

Event	Time Due	Date Due
Industry Day	N/A	May 16, 2019
Proposals Due	4:30 PM EDT	June 26, 2019
Notification of Proposal Selections	N/A	September 24, 2019

5.2 General Instructions and Information

5.2.1 Notwithstanding section 8. of BAA HSHQDC-17-R-B0002, this BAA Call (70RSAT19RB00000001) does not require, nor does the Government want, the submission of white papers. Responding to this BAA Call requires the submission of proposals as described in section 9. of BAA HSHQDC-17-R-B0002, subject to the terms specific to this BAA Call.

5.2.2 Proposals may address more than one TTA, or portions of a TTA. However, if more than one TTA is being covered, then the technical approach must describe which of the TTAs is being addressed by the different aspects of the proposed work and clearly differentiate the tasks; also, the Official Transmittal Letter required by BAA HSHQDC-17-R-B0002, 9.6.1 c., must clearly state that the proposal is responding to multiple TTAs and identify the TTAs responded to. In addition, because the DHS S&T portal does not have the capability to identify more than one TTA that a proposal can be a response to, proposals responding to multiple TTAs may be submitted into the DHS S&T portal in response to any TTA. Offerors are also free to submit multiple, separate proposals against different TTAs.

5.2.3 Offerors may provide multiple proposal submissions that address all or parts of any TTAs.

5.2.4 All software developed and delivered is required to be subject to security auditing; therefore, the offeror's technical approach must identify how security auditing will occur. Also, DHS expects offerors to follow best practices on software design.

5.2.5 The protection of sensitive information and the security of information technology (IT)

systems that process, store, or transmit sensitive information is critical to the DHS mission. IT systems are subject to threats that can compromise the confidentiality, integrity, or availability of sensitive information, which can adversely affect DHS operations, assets, and individuals. As of 2015, DHS has taken interim measures to mitigate these concerns by developing special clauses that address the safeguarding of sensitive information. Offerors are advised that these special clauses may be included in a contractual award if that award is determined by DHS to represent a high risk of unauthorized access to, or disclosure of, sensitive information. Complete information regarding this topic can be obtained by reviewing Homeland Security Acquisition Regulation Deviation 15-01⁹.

5.3 Type Classification Ceilings

Notwithstanding section 2.2. of BAA HSHQDC-17-R-B0002, Type Classifications will not be used for this BAA call. See Section 4.4 for the expected funding profile by TTA.

5.4 Proposal Submission Requirements

To be considered for award, offerors **MUST** submit a proposal, compliant with the aforementioned response dates, in accordance with the BAA HSHQDC-17-R-B0002. Submissions not in compliance with BAA HSHQDC-17-R-B0002 may be rejected (note: the cover page created by the DHS S&T BAA Portal must be included, but does not count against the page count). BAA HSHQDC-17-R-B0002, Section 9 discusses proposal preparation and describes the required proposal content; however, in addition to the guidance in HSHQDC-17-R-B0002 Section 9, the following table summarizes the proposal contents required for this BAA Call in addition to the requirements found in section 9. “Proposal Submission Requirements,” of BAA HSHQDC-17-R-B0002:

Volume	Volume Title	Page Limit	Content Subject to Page Limit	Content Excluded from Proposal Page Limit
1	Technical Proposal	25	<ul style="list-style-type: none"> • Proposal Abstract • Detailed Technical Approach • Target Capabilities • Go/No Go evaluations • Statement of Work, Schedule, and Milestones • Quad Chart 	<ul style="list-style-type: none"> • Cover Page (1 page) • Transmittal Letter (1 page) • Data Management Plan (2 pages) • Data Rights Assertions (No page limit)
2	Price/Cost Proposal	(None)	(N/A)	N/A

5.4.1 Content excluded from the page limits above will count against the page limit if the individual page limits are exceeded, e.g., a Transmittal Letter that is two (2) pages long will count as one (1) page against the proposal page limit.

5.4.2 While the Price/Cost Volume does not have a page limit, offerors must follow the

⁹ https://www.dhs.gov/sites/default/files/publications/HSAR%20Class%20Deviation%2015-01%20Safeguarding%20of%20Sensitive%20Information_1_0_0.pdf

guidance in BAA HSHQDC-17-R-B0002, section 9.6.2 regarding its preparation, formatting, and content.

5.4.3 The information outlined in Section 5.5 below must also be included in any submitted proposal.

5.4.4 Subcontractor Cost Submission: Referencing, BAA HSHQDC-17-R-B0002, Section 9.6.2.b.(6), if the subcontractor costs cannot be included with a prime's detailed cost breakdown, then the prime contractor must stipulate on the detailed cost breakdown that the costs presented only represent those from the prime and the subcontractor's costs are provided separately as an attachment to an e-mail sent to MNI19-BAA-Call@hq.dhs.gov. The subject line of the email shall say "Separate Subcontractor Cost Submission – [insert the proposal number assigned from the DHS S&T BAA Portal]". The body of the email shall contain the following:

- 1) The prime entities name which should be the same entity that is registered in the BAA portal;
- 2) A POC (name and phone number) from the prime entity; and
- 3) For each subcontractor proposal attached, include:
 - a. The name of the subcontractor for the subcontractor proposal attached; and
 - b. A POC (name and phone number) from the subcontractor whose proposal is attached.

The separate subcontractor cost proposal must be as detailed as the Offeror's cost proposal and must be received at the location designated in the individual solicitation no later than the closing date and time specified by the solicitation. Note that email transmission time may vary depending on the file size of the attachment(s) included in the email. Therefore, ensure there is adequate time for receipt of the email and any accompanying attachments of the subcontractor(s) cost proposal(s) by the required closing date and time. Acceptance of the email submission is dependent upon the actual date and time the e-mail and any accompanying attachment(s) is RECEIVED by the in-box for MNI19-BAA-Call@hq.dhs.gov. **NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE. ANY SUBCONTRACTOR COST PROPOSAL RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE WILL RESULT IN THE PROPOSAL OF WHICH IT IS A PART BEING FOUND TO BE LATE AND THE PROPOSAL WILL NOT BE EVALUATED.**

5.5 Special Submission Technical Requirements for Proposals

All proposals, unless otherwise noted, must address the following requirements:

5.5.1 Proposals must define the Target Capabilities consisting of technical and operational capabilities that the developed solution will provide. The Target Capabilities must be identified for each proposed Go/No-Go period in discrete measurable metrics. The proposal should also discuss a plan or outline on how the metrics and analytic techniques will evolve to accomplish the proposed work.

5.5.2 Propose Go/No Go evaluations using the aforementioned Target Capabilities.

5.5.3 Propose a 6 month pilot as a fully-priced option. While the option will be dependent on identification of an interested DHS entity, Federal government, or HSE partner, offerors should plan for a monthly level of effort similar to the base effort and factor in delivering updated deliverables. Performance of the option will be defined by the Statement of Work and Pilot Demonstration Plan; the final version of the Pilot Demonstration Plan must be approved by the Government. The Pilot Demonstration Plan must detail one or more pilots, a revision process for software and documentation, installation requirements, and pilot results.

5.5.4 Data Management Plan. All proposals must include a data management plan (DMP). The DMP should be no more than two pages and must be included at the end of Volume 1. The DMP does not count toward the page limit in the technical volume and is required to address the following:

- The types of data, metadata, samples, physical collections, software, curriculum materials, and other materials to be collected and/or generated in the course of the project;
- The standards to be used for data and metadata format and content;
- The physical and/or cyber resources and facilities (including those supplied by third parties) that will be used to store and preserve the data;
- The policies for access and sharing including provisions for appropriate protection of privacy, confidentiality, security, intellectual property, or other rights or requirements;
- The policies and provisions for re-use, re-distribution, and the production of derivatives.

The DMP should reflect best practices in the relevant research community and be appropriate for the data to be generated as part of the proposed activities.

Definition:

As noted in the Code of Federal Regulations (2 CFR 215.36), "research data" is defined as:

"the recorded factual material commonly accepted in the scientific community as necessary to validate research findings, but not any of the following: preliminary analyses, drafts of scientific papers, plans for future research, peer reviews, [or] communications with colleagues. This "recorded" material excludes physical objects (e.g., laboratory specimens)."

This definition includes not only original data but also "metadata" (e.g., experimental protocols, software code written for statistical or experimental analyses or for proofs-of-concept, etc.).

Additional Guidance for DMP Content:

The DMP should clearly articulate how the offeror plans to manage and disseminate data generated by the project. The plan should outline the rights and obligations of all parties as to their roles and responsibilities in the management and retention of research data. It should describe how the research team plans to deposit data into any relevant and appropriate disciplinary repositories (e.g., see <https://www.impactcybertrust.org> and <https://continuousassurance.org>) that are appropriately managed and that are likely to maintain the metadata necessary for future use and discovery.

The DMP should describe the types of data, metadata, scripts used to generate the data or metadata, experimental results, samples, physical collections, software, curriculum materials, or other materials to be produced in the course of the project. The plan should then describe the types of data to be retained, managed, and shared, and the plans for doing so. The DMP should cover the following, as appropriate for the project:

- the period of time the data will be retained and shared;
- how data are to be managed, maintained, and disseminated;
- factors that limit the ability to manage and share data, e.g., legal and ethical restrictions on access to human subjects data;
- provisions for appropriate protection of privacy, confidentiality, security, and intellectual property;
- mechanisms and formats for storing data and making them accessible to others, which may include third party facilities and repositories; and
- other types of information that would be maintained and shared regarding data, e.g. the means by which it was generated, detailed analytical and procedural information required to reproduce experimental results, and other metadata.

5.6 Foreign Participation

Offerors are reminded that foreign participation may occur as defined in BAA HSHQDC-17-R-B0002 (current issue) Section 1.3. Therefore, offerors should provide unit costs for any deliverable not anticipated for delivery in a softcopy format.

5.7 Export Control Requirements

Offerors are reminded of the export control markings required by BAA HSHQDC-17-R-B0002 (current issue) Section 9.6.1 t.

5.8 Travel

Travel will be required from the contractor site to Washington, DC two times per year for 2 people for 2 days each. This travel will be used for program reviews and stakeholder meetings. In addition, there will be two events per year (e.g., RSA Conference and Mobile World Congress Los Angeles) in San Francisco and Los Angeles. Therefore cost estimates should include travel from the contractor location to San Francisco and Los Angeles for 2 people for three days. For all the travel, projects will be required to provide a briefing, typically 20 minutes, and are strongly encouraged to provide demonstrations when appropriate.

5.9 Industry Day

Registration for the industry day for this BAA Call must be completed using the following link: <http://www.cvent.com/d/w6qv3j>

While not required, registration for and attendance at the industry day is highly encouraged.

5.10 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (70RSAT19RB00000001) must be

emailed to MNI19-BAA-Call@hq.dhs.gov no later than 4:30 PM EDT on June 12, 2019. Emails submitting questions are to include "Questions for SRMNI BAA Call" in the subject line. Questions will only be accepted and answered electronically.

5.11 Order of Precedence

In the event that any of the terms and conditions contained in this solicitation conflict with terms and conditions included in BAA HSHQDC-17-R-B0002 (current issue), the terms and conditions in BAA HSHQDC-17-R-B0002 shall take precedence.

5.12 Evaluation Criteria

Consistent with BAA HSHQDC-17-R-B0002 section 11, the evaluation criteria to be used for the peer/scientific review of proposals received in response to this Call is identified below in descending order of importance:

a. **Criterion I: Responsiveness to Technical Topic and Technical Approach.**

The potential of the proposed technology/solution for meeting the project goals provided in BAA call will be assessed. Also, the technical and managerial approach to the proposed work will be assessed, and evaluations may address any one, or more, of the following: including: an assessment of the technical development methodology to achieve the project goals of the BAA call; an assessment of how the development will be managed possibly including any relevant risks, mitigations, dependencies, and milestones; and an assessment to determine whether the if task descriptions are complete and in a logical sequence; and if, with all proposed deliverables clearly defined.

b. **Criterion II: Offeror's Capabilities and Related Experience.**

The offeror's prior experience in similar efforts will be assessed to determine if the offeror clearly demonstrates an ability to deliver products that meet the proposed technical performance within the proposed budget and schedule. In addition, the proposed team will be reviewed to determine whether the personnel have the expertise to perform the proposed work as well as the ability to manage the project cost and complete the project within the proposed schedule.

c. **Criterion III: Transition Approach.**

As technology adoption is a major DHS/S&T goal for R&D projects, a qualitative assessment will be made regarding how the proposed technology/solution will be transitioned to an operational user (e.g., commercialized or used by a DHS component). The assessment will determine the likelihood that the offeror will be able to deploy a technology and/or solution(s) that can be transitioned effectively to operational use either through commercialization of the technology, open source distribution, or through other means. Because intellectual property rights will impact technology transition, an assessment will be made of software/data to be included in the proposed technology for which the Government would not receive unlimited rights (as identified in the Assertion Table included with the proposal). The assessment will consider:

- (1) proposed use(s) of the software/data;
- (2) the explanation as to how the Government will be able to reach its technical goals (including transition) within the proprietary model offered; and
- (3) the nonproprietary alternatives in any area that might present transition difficulties or increased risk or cost to the Government under the proposed proprietary solution.

d. Criterion IV: Cost

The cost evaluation factor for proposals is as follows:

Cost Reasonableness and Cost Realism. The proposed costs are reasonable (i.e., reflect a sufficient understanding of the technical goals and objectives of the solicitation, and are consistent with the offeror's technical/management approach (to include the proposed SOW)), and are based on realistic assumptions. The costs for the prime and subcontractors/consultants 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).

The primary basis for selecting proposals for award shall be technical importance to agency programs.

DHS S&T reserves the right to select for award and to fund all, some, or none of the proposals received in response to this BAA Call.

5.13 Assertion of Data Rights

(1) Offerors are reminded that failure to include the Assertion of Data Rights information required by BAA HSHQDC-17-R-B0002, Section 9.6.1 u., will result in a proposal being deemed non-compliant and therefore not reviewed or considered for funding.

(2) It is anticipated that the proposed Assertion of Data Rights will be incorporated in the resultant award instrument. To this end, proposals must include a severable Assertion of Data Rights (i.e., it will begin on a new page and the following section shall begin on a new page) without any proprietary restrictions, which can be removed from the proposal and attached to the contract or agreement award. After proposal submission, any changes to this information requested by an Offeror may cause a proposal to be re-evaluated or deemed not selectable at the Government's discretion. The format for this section is as follows:

Assertions Table

Identify in the table below each deliverable included in the Offeror's proposal. For each deliverable listed in the below table identify any assertion of restriction on the Government's Use, release or disclosure of technical data or computer software.

Deliverable	Technical Data or Computer Software to be Furnished With Restrictions*	Basis for Assertion**	Asserted Rights Category***	Name of Person Asserting Restrictions****

*For technical data (other than computer software documentation) pertaining to items, components, or processes developed at private expense, identify both the deliverable technical data and each such item, component, or process. For computer software or computer software documentation identify the software or documentation.

**Generally, development at private expense, either exclusively or partially, is the only basis for asserting restrictions. For technical data, other than computer software documentation, development refers to development of the item, component, or process to which the data pertain. The Government's rights in computer software documentation generally may not be restricted. For computer software, development refers to the software. Indicate whether development was accomplished exclusively or partially at private expense.

If development was not accomplished at private expense, or for computer software documentation, enter the specific basis for asserting restrictions.

***Enter asserted rights category (e.g., government purpose license rights from a prior contract, limited, restricted, or government purpose rights under this or a prior contract, or specially negotiated licenses).

****Corporation, individual, or other person, as appropriate, or enter "none" when all data or software will be submitted without restrictions.

Completed by:

Signature
Printed Name and Title

Date