

**Broad Agency Announcement Solicitation HSHQDC-17-R-00059
Version 19-BABC May 22, 2017, 2017 PARADINE BAA 1**

Project: Application of Network Measurement Science: Predict, Assess Risk, Identify (and Mitigate) Disruptive Internet-scale Network Events (PARADINE)

1. Introduction

1.1 This BAA solicitation (HSHQDC-17-R-00059) is a call issued against Department of Homeland Security (DHS), Science & Technology (S&T), Cyber Security Division (CSD), 5-Year Broad Agency Announcement (BAA), HSHQDC-17-R-B0002 Amendment 1. All terms and conditions of the DHS S&T CSD 5-Year BAA HSHQDC-17-R-B0002, Amendment 1, apply to this solicitation unless otherwise noted herein.

1.2 Internet attacks and disruptions often occur without much warning or many obvious precursors, and this makes both defense and attribution very difficult. Attacks on availability ramp up over seconds or minutes, and the only viable defense organizations have aside from generic protection mechanisms or heavy investment in fault tolerant, distributed, high availability infrastructure is to rely on agile response teams and other intrusion response capabilities to manually triage the event¹. At the same time, there are few generally-accepted thresholds and parameters for determining what a “disruptive” event actually is or how an organization might reliably recognize such an event as it happens or find it in pre-recorded data. In order to lay the groundwork for effective and widely-accepted scientific measurement of disruptive network events, the research and operator community must develop a shared understanding of what these parameters are, the relevant structures that define a disruptive event, and common tools and mechanisms for recognizing an instance of a disruptive event. With this shared understanding and common framework of reliable tools, the community would then be in a position to identify and possibly predict the occurrence and impact of disruptive events on a very short timescale either before they unfold or in their very early stages.

The overall Application of Network Measurement Science (ANMS) program has several major goals, each corresponding to a separate BAA. The first goal (and the focus of this PARADINE BAA) is to define, identify, produce and report operational instances of disruptive events, accompanied by attribution that captures root cause analysis. The second goal, not included in this BAA, is to predict (with attribution) emerging or unfolding Network/Internet-scale Disruptive Events (NIDEs) based on a thorough understanding of the characteristics of a variety of such events and the current Internet state. The third goal, also not included in this BAA, is to develop a risk analysis tool that supports prediction, what-if scenario exploration, and attribution. Technologies developed under these BAAs should be designed to demonstrate the ability to automatically use very early indications of attack, network instability, broader network behavior, or other domain information to understand the actual properties and details of a Network/Internet-scale Disruptive Event (NIDE).

1.3 A Basis for Reliable Identification, Prediction, and Attribution: Network Measurement Science.

Network Measurement Science is the efficient and principled application of the scientific method to network measurement. Network measurement is a hard problem given both the scale of the

Internet and the flux in behavior of connected systems. The current state of the art for Internet measurement research is that there are many individual measurement tools and techniques, such as ping, traceroute in various versions, net flow, and packet sampling from network telescopes², fast scanners³, or sensor nodes^{4,5} distributed throughout the Internet. However, data from applying measurement techniques are rarely combined for more accurate analysis, so techniques for fusing data and analysis of the fused data are not generally available.

Measuring the security properties of the Internet is challenging because while recording network data and traffic has been studied since the initiation of the Internet and resulted in common network tools and protocols, measuring meaningful security properties requires having a clear idea of Internet behavior at scale, at speed, and from multiple perspectives. Current approaches to detecting and deriving a full analysis of compromises, cyber-attacks, and Internet-scale disruptions require a good deal of manual intuition and interpretation, make the presumption that they are detecting some property of the attack event itself, and often trail the actual events by weeks, months or years⁶. In some cases, important relevant data goes uncollected and is unavailable for forensics or auditing. However, even when relevant data *is* collected, patterns emerge only after processing significant amounts of data for long periods of time. Therefore, increasing measurement efficiency and reducing measurement bias are just two possible areas for improvements of network measurements that could aid the ability to predict disruptive events and assess their impact.

2. PARADINE Project Description and Scope

2.1 Program Overview

To provide sufficient background for the overall research activities in the ANMS program and context for the specific research and Technical Topic Areas listed in this current PARADINE BAA call, this section discusses the fundamental and operational challenges that cut across all the program areas of interest. Mentions of prediction and risk assessment (the primary research topics in the second and third ANMS BAA calls, respectively) are present to provide performers with sufficient context that motivates the problem setting. Section 3 describes the activities specific to this PARADINE BAA call.

2.2 Fundamental Challenge

Traditionally, network measurement tools and techniques have been applied to data related to cybersecurity events, and these tools can increase our ability to understand what has happened, but they seldom increase our understanding of what *may* happen. **Prediction of the future behavior of a complex networked system under the influence of an unconstrained attacker is a serious challenge.** Yet, prediction in this domain must be based on solid, repeatable measurements that follow generally-accepted means of identifying the nature of disruptive events.

2.3 Benefit

The existence of reliable, automated detection can bend the asymmetric relationship between attacker and defender back toward a level playing field and offer precious minutes of response time to both adversarial and non-adversarial events. Arguably, minutes of warning saves lives in

cases involving natural disasters such as tornadoes. A few minutes warning could offer the same kind of benefit for cyber-physical systems, especially those in critical infrastructure settings.

2.4 ANMS BAA Calls

This PARADINE BAA call is the first in a series of three that seeks to apply Network Measurement Science for Internet Measurement, to define, identify, predict and use measurements for Network/Internet-scale Disruptive Events (NIDES), then use NIDES (and their predictions) in a tool for risk assessment, and to do this as quickly as possible, “near-real-time”. Development of accurate attribution for NIDES is included in all three BAAs. Figure 1 depicts the relationship of this BAA call to potential future BAA calls, where an overview of the plan for each is as follows:

2.4.1 This BAA call focuses on the definition and identification of NIDES, including reporting and attribution. Performers should anticipate how their NIDE identification, production, and attribution techniques might help feed into predictive methods and risk assessment. Performers are required to provide an Application Programming Interface (API) that allows the results of this work to be shared and incorporated into the efforts below or other external tools or analysis processes.

2.4.2 The second BAA call could focus on prediction of NIDES, including methods to dynamically adjust attribution hypotheses during event prediction. Methods of interest include those that attempt to forecast the occurrence of NIDES from initial conditions, rapidly predict subsequent events during an unfolding NIDE, analysis of how existing disruptions and Internet dependencies might play out in future events, and validation of those techniques in realistic settings or on real traffic.

2.4.3 The third BAA call could focus on the creation of a risk assessment tool that will provide mission impact assessment, a simulation environment for “what-if” scenario exploration capability, attack design, attack mitigation strategies, and an API to a SIEM (Security Information and Event Management) or similar tool to send alerts for malicious events identified by the tool. This will include the integration of information generated by the results of 2.4.1 and 2.4.2. This will provide the necessary information for decision makers to more effectively allocate limited resources to protect systems and networks affected by NIDES, and will also entail exploration of both technical and policy mechanisms related to attribution.

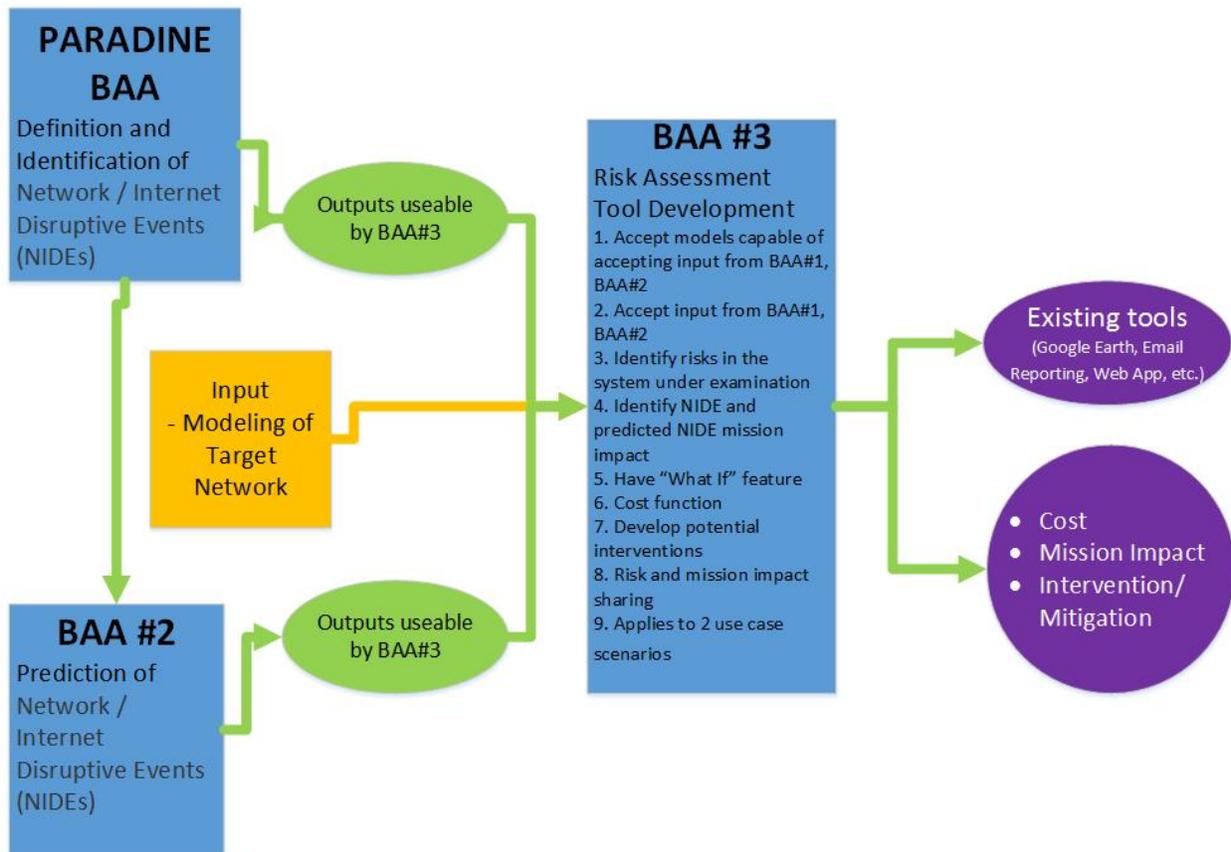


Figure 1. Diagram of relationship between ANMS PARADINE BAA, BAA #2, and BAA #3. Outputs from PARADINE BAA and BAA #2 (green), as well as inputs from modeling of the network under assessment (gold) produce outputs (green) to existing tools.

2.5 Definition of “Disruptive”

A disruptive event in a network is an event that causes a material loss or degradation of service, a material reduction in resilience, or manipulation of traffic flows with adverse consequences. It may involve complete or partial degradation of availability on a set of links by increasing latency or decreasing available bandwidth. It might involve attacks on the integrity of the network messages themselves. Disruptive events in the cyber realm can have an impact on public safety in the physical world and vice versa. Disruptive events occur for many reasons, such as natural causes, human error, and cyberattacks. Examples include storms, such as superstorm Sandy⁷ in the fall of 2012, solar flares, earthquakes⁸ or Tsunamis⁹, cable cuts¹⁰ (depending on the volume of the service disruption)¹¹, government policy restrictions¹², cyber-attacks such as ransomware¹³ or other malicious software¹⁴, or Distributed Denial of Service (DDoS)¹⁵ attacks. A disruptive event, therefore, has both static and dynamic aspects: it relies partially on the fixed (or at least stable) attributes of the network topology (such as physical locations of transmission links along rights-of-way) and the dynamic attributes of an unfolding event in both the physical world and the networked computing environment. This information can be observed with respect to multiple communication layers and multiple types of networking environments or services, including cellular, other wireless technologies, broadband, and VoIP (e.g., TDoS or DDoS)).

Creating a definition of a NIDE amounts to specifying a methodology for using both

observations of these static properties and observations of the impact the event has on dynamic data sources, such as traces of Internet traffic or records of topology changes. The goals of the Technical Topic Areas (TTAs) listed below describe a set of properties, templates and a *method* that could specify how to recognize and report on a NIDE from a diverse set of information.

2.6 Operational and Research Challenges for Network Analytics of Disruptive Events

The difficulty of identifying, reporting, and attributing how a disruptive event will unfold is compounded by the ongoing evolution of Internet technologies, including IPv6 addressing and related protocols, pervasive cellular and broadband connectivity, and the increased use of opportunistic encryption, strong authentication protocols, and anonymity (thereby complicating efforts at measurement and attribution).

Although good trace filtering tools exist and significant effort has been spent to create large, shareable repositories of Internet and network security data, aggregation tools and data fusion can take on the order of weeks or months to process their data collections, particularly if processing involves checking live network state or issuing new queries to data sources. As a result, most current analysis occurs on a time scale that is retrospective. In addition, transient disruptions can go unnoticed and therefore cannot contribute to efforts that look at larger cyber situational awareness and risk analysis.

Furthermore, there is a fundamental tension between the power of data analytics and the need to tamp down or suppress the activity of data collection mechanisms (e.g., ping, traceroute) that query systems across the network owned by third parties. Aggressive data collection can bring high-quality, timely, and high-value information to analysis tools, but runs the real risk of being cut off, filtered, or banned via blacklisting.

Several challenges to overcome for the ANMS Program and the Technical Topic Areas of the PARADINE project include:

Dynamic Adaptive Fusion – important insights can be gleaned from fusing multiple sources of data in a dynamic, interactive fusion, including launching probes and measurement queries based on evolving, real-time data as well as during processing of previously-captured data traces. There is a need for information collection mechanisms that adapt to the changing conditions of the network under examination and help foresee how the measured properties might impact subsequent predictive analysis.

Speed – Since the overall goals of PARADINE include timely identification, reporting and predictions and attribution of NIDEs, achieving determinations (classification, matching, identification and reporting of a candidate NIDE) at speeds that outpace current tools by at least an order of magnitude are of interest. To be effective, identification, production, and reporting should happen on the order of tens of minutes or less.

Fidelity – To be effective, NIDE identification, attribution, and predictions should be meaningfully tied to the real world. Models that drive the risk management tool must be based on high-fidelity representations of a composition of both physical and IT components. In addition, NIDE identification profiles must be of high enough quality and specificity to capture the dependencies between network components and realistic thresholds for triggering the

identification of an event.

2.7 Disruptive Event Scenarios

The context for the following examples is a Smart City¹⁶, where information and communication technology (ICT) and Internet of Things (IoT) solutions are integrated in a secure fashion to manage a city's assets. The city's assets include, but are not limited to, city departments' information systems, such as schools, libraries, transportation systems (such as airports, river ferries, or trains), hospitals, power plants, water supply networks, waste management, law enforcement (including ground, water and air), and other community services. The following examples are disruptive events on the Internet that are of interest to this BAA call. Technical approaches should describe an analytic framework to address these, and yet has the flexibility to address to other types of internet disruptions that have not been mentioned in this BAA call.

2.7.1 A NIDE that causes a set of Classless Inter-Domain Routing (CIDR) block to be off line. This could affect the entire city, or only a portion of it.

2.7.2 A NIDE that impacts communication. Nearly all communication in the Smart City will involve the Internet in some way, such as VoIP phones, land lines or cell phones (that start at a tower) that migrate to the Internet, or social media (Twitter, Facebook, etc.). Business communications utilize email (both internal to an enterprise as well as external), video conferencing, web sharing (e.g. WebEx, skype) and other electronic communications.

2.7.3 A NIDE that impacts public transportation. This could be anything from city buses, trains or light rail, water craft such as ferries, or aircraft and airports.

2.7.4 A NIDE that impacts public utilities, such as water treatment plants, city electrical or natural gas service, etc.

2.7.5 A NIDE that disrupts financial services, such as home banking, stock exchanges or commodity exchanges,

2.7.6 A NIDE that impacts exchange of expertise. Often technical expertise and demand for that expertise are in geographically diverse areas. Examples include remote medicine (diagnosis, monitoring) and telework (e.g. teaching, computer programming).

2.7.7 A NIDE impacting Public Safety. This could include Public Safety Answering Point (PSAP) operation, telephone denial of service at hospital emergency rooms or intensive care units, first responder communications or public safety announcements.

2.7.7.1 One example of public safety announcements is the Virtual buoy system. In both inland and coastal waters, virtual buoys are used to broadcast the exact location of hazards, such as sand bars that move fairly often. This enables updating the information in software rather than physically moving a device. The cost of providing new buoys is also minimized, since a physical buoy does not need to be manufactured and placed at the location of the hazard. A scenario where a NIDE impacts buoy position, buoy sensors, and buoy communications could occur.

2.7.7.2 New Public Safety Vehicles or Equipment. As new public safety equipment is developed, many features that were previously analog or did not exist at all are now digital. This could include ships for water rescues, automobiles, light trucks or sport utility vehicles for law enforcement use, firetrucks, emergency housing during disasters (campers or trailers), etc. All digitally enabled systems need protection from NIDEs. These include SCADA (Supervisory Control and Data Acquisition) systems, GPS, body cameras, drones, and a myriad of IoT devices associated with public safety functions. A NIDE scenario could occur that could impact the operation of these systems or technology.

3.0 Technical Topic Areas (TTAs)

In this PARADINE BAA call, DHS is interested in developing innovative technology that supports high-quality identification, classification, description, attribution and reporting of disruptive Internet events. This work will help inform and feed into later efforts focused on both (1) prediction and early warning of impending attacks and similar events and (2) high-fidelity risk assessment modeling and risk management in anticipation of significant cyber-attacks on critical infrastructure, described in the aforementioned disruptive event scenarios. This first BAA call has two TTAs, below, that are intended to develop products that are useful as standalone methods and artifacts, and yet could be integrated into solutions that would eventually meet the second and third goals of the program, not covered by this BAA call, focusing on prediction and risk assessment, respectively. Attribution and root cause analysis are integrated into each of the PARADINE goals, as potential precursors for future developments. Also, an overarching goal of this BAA call is that performers will collaborate and create open products that will support the aforementioned future ANMS developments, as well as support the interaction depicted in Figure 2.

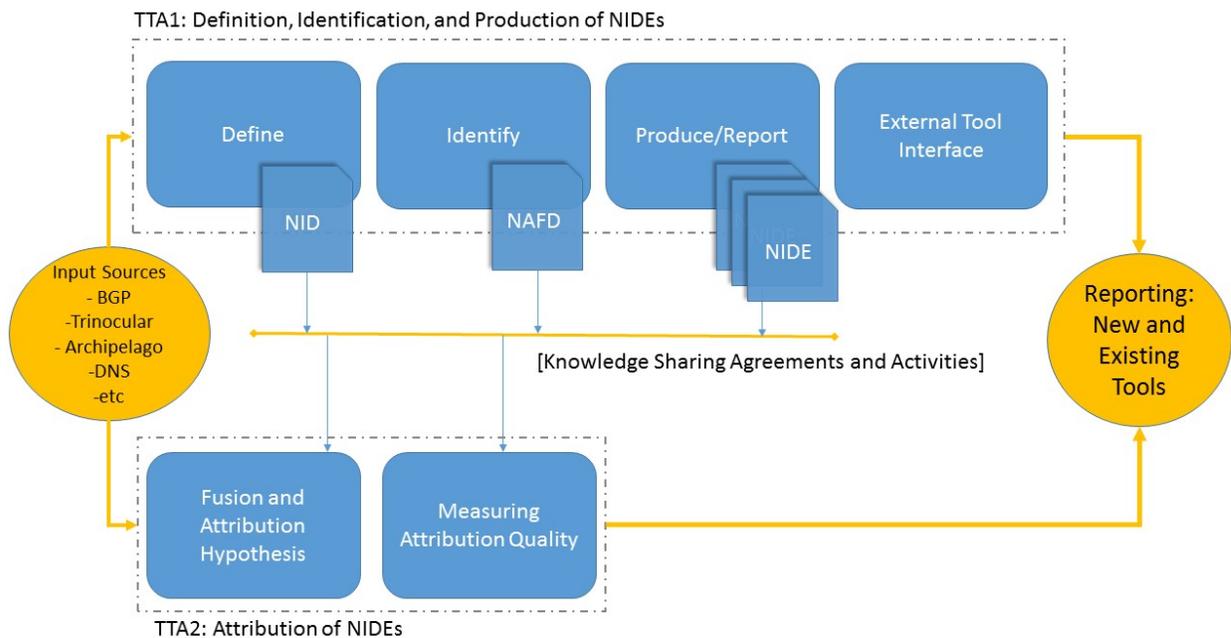


Figure 2. TTA1 and TTA2 use existing data sources to identify and attribute disruptive events. TTA1 focuses on methods for defining these events and finding instances of them. TTA2 focuses on developing attributions for these events.

3.1 TTA #1: Definition, Identification, and Production of Network / Internet Disruptive Events (NIDEs)

This TTA intends to generate an approach to sensing, quantifying, and categorizing Network/Internet-scale Disruptive Events (NIDEs) by constructing definitions and applying them to identify instances of NIDEs. For consistency, repeatability, and correctness, technical approaches should describe a method of defining NIDEs that encompass NIDE attributes described in Section 2.5 and 2.6. NIDE production encompasses specifying algorithms that use the NIDE structure definitions to identify NIDEs in existing or new data and research testbeds. As a result, deliverable requirements include algorithms, a collection of data with evidence of NIDEs, and reports summarizing the efficacy of applying the proposed NIDE structure definition (including pointing out any gaps that make NIDE identification difficult or infeasible). Production-ready code for identification and reporting of NIDEs is a desired outcome for this TTA. Specific goals for this TTA are as follows:

3.1.1 TTA #1 Goal 1 - NIDE Identification Document (NID). The first goal for this TTA is to define a Network/Internet-scale Disruptive Event (NIDE) in terms of quantifiable metrics and classifications, as well as documenting required sensors and data to measure the NIDEs, and produce a NIDE Identification Document (NID). The NID must fully define the taxonomy for classifying NIDEs and provide context to explain the development approach as well as the relationship of the NIDE classifications to NIDE scenarios. For example, although it is clear when some events disrupt Internet service, this is not always the case. When a hurricane takes out the infrastructure of an area, it is clearly a disruptive event. A NID will address the parameters needed to identify and quantify that a NIDE has occurred, perhaps by defining the number of consumers that were disconnected from the Internet and the length of time for the disruption. Other applicable causes of NIDEs could be: cable cuts, or BGP hijacking events such as when traffic from one country is maliciously routed through another country. Another consideration applicable to NIDE definition could be an event when service is degraded but not completely cut off. The goal of the work in this part of TTA #1 is not so much to offer an authoritative general definition of incidents such as DDoS, but rather to identify reliable defining characteristics of such events, that will lay the foundation for a common framework for defining disruptive events and scientifically and empirically determining ranges of values for NIDE attributes (e.g., m minutes of p% drops for networks of scale S).

3.1.2 TTA#1 Goal 2 – NIDE Analysis Framework Document (NAFD). The second goal of the TTA is to develop an analysis methodology and techniques to sense and identify NIDEs, preferably for identification in near-real-time, and document the results in a NIDE Analysis Framework Document (NAFD). Technical approaches should consider data inputs required to identify NIDEs based on NIDE scenarios. A relevant approach could address varied data inputs from a single source to fusing data from many sources. Examples of monitoring infrastructures include: Trinocular (<https://ant.isi.edu/bib/Quan13c.html>) – an edge network monitor; BGPmon (<http://www.bgpmn.io/>) – a tool that monitors BGP routes; Internet Atlas (<http://internetatlas.org/>) - a tool providing the physical representation of the Internet; the FCC Measuring Broadband in America (MBA) for measuring consumer broadband performance; and Archipelago (<http://www.caida.org/projects/ark/>) an Internet topology monitoring tool. The state-of-the-art is that it takes days to months to get analysis results from the currently available tools, and even when analysis becomes available it is usually based on a single data source. Another potentially complimentary approach to the problem could be combining information

from the data and control planes, which would provide a higher level of confidence and detection precision, especially if there was an independent confirmation of a NIDE available in the observations from each source. Regardless of the approach to data fusion, the approach should identify many types of NIDEs, some that are not detectable when using a single data source. Technical approaches must address how this goal will be met by discussing the data sources that would be fused, as well as how the elements from each source relate to the other sources used to yield an aggregate result.

3.1.3 TTA#1 Goal 3 – Production and reporting of NIDEs. The third goal of this TTA is to produce reports identifying actual occurrences of NIDEs in near real time. Performers should build on the capabilities from Goals 1 and 2 (definition, documentation, and design) to implement algorithms and tools capable of identifying NIDEs. Performers will deliver these tools, instances of NIDEs detected, and reports on the feasibility and efficacy of this identification. The reports should specifically identify gaps, technical shortcomings, or obstacles to completing automated, near-real-time NIDE identification (such obstacles might include, but are not limited to: whether this is due to inadequate data fusion, resource constraints affecting the feasibility of real-time processing, scale challenges, incomplete data). The deliverables associated with this goal are NIDE Analysis Reports.

3.1.4 TTA#1 Goal 4 – NIDE Analysis Tools Interface. Building on the NID and NAFD from the first and second goals, this last goal is to create an interface to serve as a data source to NIDE analysis tools. The deliverable associated with this goal is a NIDE Framework Interface. The NIDE Framework Interface should be an API and associated developer documentation. In addition, given that there is not a single standard format for sharing this type of data or analysis, offerors are encouraged to enhance existing standards or techniques rather than create an entirely new standard; and technical approaches must justify the sharing approaches.

3.2 TTA 2: Attribution of Network / Internet Disruptive Events

Associating identities and root causes with a NIDE is a problem that entails developing methods that support comprehensive root cause analysis and new attribution techniques for disruptive events. Attribution techniques should produce an identifier (this might be a multi-dimensional artifact, not just a simple string or name) and a metric for attribution quality (i.e., some judgement of the confidence of the attribution procedure or the amount of confidence in the sources of information used to derive it). Attribution should be seen as one property of a NIDE and an attempt at identifying the systems, locale, or other originator of an event. For this TTA, novel attribution techniques are not meant to produce a detailed legally-justifiable personal identification or jump the gap between the cyber and human identity, although this is a desired outcome if feasible. Specific goals for this TTA are as follows:

3.2.1 TTA#2 Goal 1 – Create methods and tools for performing attribution of NIDEs. Using publically available data sources, novel and efficient attribution of these events is of interest, particularly where multi-source data fusion can assist in developing a strong hypothesis for a root cause analysis. Such attribution should be able to encompass both simple triggering conditions involving a single event (e.g., a BGP misconfiguration or an undersea cable cut) as well as activities distributed in time and space. Notably, such analysis may involve attribution of several coordinated root causes or entities. Note: Proprietary data sources may be used if available. The deliverables associated with this goal start with creation of a NIDE Attribution Methodology

Document (NAMD), which will document the concept of how attribution will be applied to NIDES including documenting required characteristics or meta-data. Using the NAMD, the next deliverable will be a study that implements the NAMD (“NAMD Study”). The study will need to document the data sources, analysis, and application of the NIDE Application Methodology to the study. Progressing, the NAMD Study serve as a basis to automate the NAMD (“NAMD Automation Suite”) and identify requirements for where tools and algorithms should be applied to NIDE attribution, as well as a Concept of Operations (CONOPS). The NAMD Automation Suite will then be used for NIDE attribution analysis. Ultimately, the objective of this goal is to automate as much NIDE attribution analysis as possible, while accounting for where human analysis is required.

3.2.2 TTA#2 Goal 2 – NIDE attribution quality analysis. Perfect attribution may be difficult or impossible to determine for any given incident, so attribution artifacts should accommodate varying degrees of detail and provide a metric expressing the quality of the attribution. For NIDES where a determination of attribution is not possible, an explanation of the gaps or obstacle should be provided. This goal will serve as a validation of the NAMD and will document a metrics-based approach to expressing attribution confidence. The deliverables associated with this goal includes a report analyzing the study implementing the NAMD, and then subsequent analyses of NAMD automation.

4. Project Structure

Section 5 includes a depiction of 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 12 month intervals (excluding the Transition/Pilot Option). The optional Pilot Task for an additional 12 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 Transition/Pilot option would only be exercised after the successful development and identification of an interested DHS entity, Federal Government partner, or partner within the Homeland Security enterprise. 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 on or about one month following 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 12 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 occur based on the Go/No-Go determinations.

Finally, project status deliverables are defined in 4.1. The key deliverables are described for each TTA below in 4.2 and 4.3. Offeror technical and managerial approaches are required to define deliverable timelines, version iteration frequency, and format for each deliverable as well as associated milestones and decision points that may not be addressed by Go/No-Go decisions. Further, in general, it is expected that the PARADINE development will be iterative.

4.1 Project Status Deliverables

The following project status deliverables are required throughout the period of performance for all PARADINE awards:

DELIVERABLE	DUE DATE
Presentation Materials from Project Meetings	Within five (5) days of presentation
Monthly Technical and Financial Status Reports	Starting on the fifteen (15) day of the month, beginning in the calendar month after award, and the fifteen (15) day of each month thereafter throughout the period of performance.
Program Reviews	Quarterly
Final Report	End of Period of Performance

4.2 TTA #1 Key Deliverables

The key deliverables for TTA #1 are defined as follows:

DELIVERABLE	DUE DATE
Target Capabilities Document	60 days after award and frequency of subsequent version iteration frequency, and format are an Offeror discretion
NIDE Identification Document (NID)	90 days after award and frequency of subsequent version iteration frequency, and format are an Offeror discretion
NIDE Analysis Framework Document (NAFD)	90 days after award and frequency of subsequent version iteration frequency, and format are an Offeror discretion
NIDE Analysis Reports	Initial delivery and frequency of subsequent version iteration frequency, and format are an Offeror discretion
NIDE Framework Interface and Documentation	Initial delivery and frequency of subsequent version iteration frequency, and format are an Offeror discretion
Go/No-Go Plan	10 months after award or option period
Go/No-Go Demonstration	10 – 11 months after award or option period
Go/No-Go Report	12 months after award or option period

4.2 TTA #2 Key Deliverables

The key deliverables for TTA #2 are:

DELIVERABLES	DUE DATE
Target Capabilities Document	60 days after award and frequency of subsequent version iteration frequency, and format are an Offeror discretion
NIDE Attribution Methodology Document (NAMD)	90 days after award and frequency of subsequent version iteration frequency, and format are an Offeror discretion
Study to Implement the NIDE Attribution Methodology Document (NAMD)	90 days after award and frequency of subsequent version iteration frequency, and format are an offeror discretion
NIDE Attribution Quality Analyses	Initial delivery and frequency of subsequent version iteration frequency, and format are an offeror discretion, but must coincide NAMD Studies
NAMD Automation Suite including CONOPS	Initial delivery and frequency of subsequent version iteration frequency, and format are an offeror discretion, but must coincide NAMD Studies
Go/No-Go Plan	10 months after award or option period
Go/No-Go Demonstration	10 – 11 months after award or option period
Go/No-Go Report	12 months after award or option period

4.3 Pilot Deliverables

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

DELIVERABLES	DUE DATE
Pilot Program Plan	30 Days after award of Pilot Option

5. Project Schedule/Milestones

A notional project schedule is shown in Figure 3, below, including anticipated meetings and demonstrations.

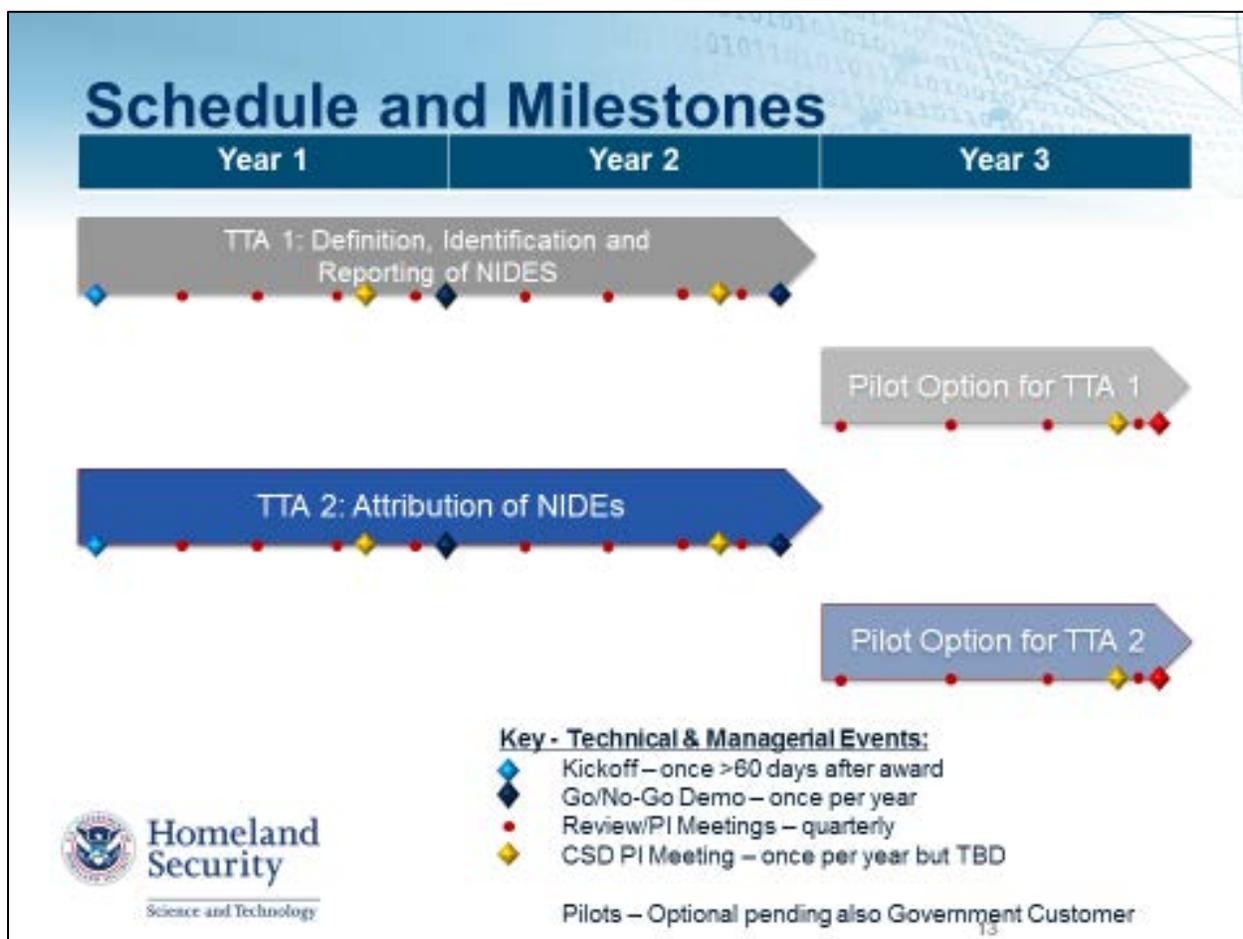


Figure 3. PARADINE. Schedule and Milestones

6. Special Instructions/Notifications

6.1 Response Dates

Event	Time Due	Date or Date Due
Industry Day	N/A	May 25, 2017
Proposals Due	4:30 PM EDT	July 14, 2017
Notification of Proposal Selections	4:30 PM EDT	September 15, 2017

6.2 General Instructions and Information

6.2.1 This BAA solicitation/call (HSHQDC-17-R-Bxxxx) **does not include a requirement for white papers** and only requires the submission of proposals subject to the date identified in the “Response Dates” table above.

6.2.2 Proposals may address more than one TTA, or portions of TTA#1. 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 both TTA #1 and TTA #2, or which portions of TTA#1. 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 both TTAs may be submitted into the DHS S&T portal in response to either TTA.

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

6.2.4 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 and encourages the use of the DHS Software Assurance Marketplace [17].

6.2.5 DHS has a strong preference for open source licensing of software for all software developed and delivered and the licenses for all proposed software deliverables will have to be identified in submitted proposals. In addition, all developed APIs are required so be released with an open source license and associated documentation are required to have an open or free copyright.

6.3 Type Classification Ceilings

Type classifications will not be used for this BAA call. However, DHS expects to make Individual awards with a 2 year period of performance and funding ranging up to \$1,000,000.00 annually.

6.4 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 Section 9, the following special instructions are added:

6.4.1 The maximum number of pages for Volume 1 is 25 pages.

6.4.2 The information outlined in Section 6.9 below must also be included in any submitted proposal.

6.4.3 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 CSD-2017-BAA@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 CSD-2017-BAA@hq.dhs.gov. **NO SEPARATE SUBCONTRACTOR COST PROPOSALS RECEIVED WILL BE ACCEPTED IF RECEIVED AFTER THE AFOREMENTIONED PROPOSAL DUE DATE.**

6.5 Special Submission Technical Requirements for Proposals

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

6.5.1 Proposals must provide a technical approach to at least two of the disruptive event scenarios from 2.7.

6.5.2 Technical approaches for TTA #1 are required to describe how their approach to NIDE definition is flexible enough to capture different types of NIDEs and demonstrate that capability by identifying a variety of real NIDEs that take place on the Internet or research testbeds. In the simplest case, a NIDE definition would help a researcher identify a NIDE in a network traffic trace and allow others to reproduce that identification using the shared description (because they would agree, for example, on the set of degradation metrics such as packet loss, latency increase, data corruption).

6.5.3 Proposals must define the Target Capabilities consisting of technical and operational capabilities that the developed solution will provide. The proposal should discuss a plan or outline on how the metrics and analytic techniques will evolve to accomplish this work.

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

6.5.5 Propose a 12 month pilot. Parameters for the optional Pilot Task for an additional 12 months. While the option will be dependent on identification of an interested DHS entity or Federal Government or Homeland Security Enterprise partner, offeror's 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 Pilot Program Plan, the final version of which must be approved by the Government. The Pilot Program Plan must detail one or more pilots, a revision process for software and documentation, installation requirements, and pilot results.

6.6 Travel

6.6.1 DHS Cyber Security Division holds an annual PI meeting where all DHS CSD funded efforts are expected to present. Projects will be required to provide a briefing, typically 20 minutes, and are strongly encouraged to provide demonstrations when appropriate. The PI meeting is typically 2.5 days and attendance at the full event is encouraged.

6.6.2 In addition to the annual DHS PI Meeting, the PARADINE Project will hold four meetings each year, two in the Washington, DC area and the others at the contractor facility.

6.7 Industry Day

An industry day for this solicitation will be held as outlined in the Federal Business Opportunities Notice which can be accessed at the following link:

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

6.8 Contractual or Technical Inquiries

All contractual or technical inquiries to this BAA solicitation (HSHQDC-17-R-Bxxxx) must be emailed to CSD-2017-BAA@hq.dhs.gov no later than 4:30 PM EDT on July 06, 2017. Emails submitting questions are to include “Questions for PARADINE BAA Call” in the subject line. Questions will only be accepted and answered electronically.

6.9 Order of Precedence

Additional Information: In the event that any of the terms and conditions contained in this solicitation (HSHQDC-17-R-00059) 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.

Footnotes:

1. <http://dyn.com/blog/recent-iot-based-attacks-what-is-the-impact-on-managed-dns-operators/>
2. https://www.caida.org/projects/network_telescope/
3. <https://zmap.io/>
4. <http://www.caida.org/projects/ark/>
5. <http://research.dyn.com/>
6. <http://www.cbc.ca/news/business/nortel-hit-by-suspected-chinese-cyberattacks-for-a-decade-1.1218329>
7. https://en.wikipedia.org/wiki/Hurricane_Sandy
8. <http://www.huffingtonpost.com/news/washington-dc-earthquake/>
9. <http://www.livescience.com/39110-japan-2011-earthquake-tsunami-facts.html>
10. <http://www.inforum.com/news/4070167-most-service-restored-after-cable-cut-causes-phone-internet-outages-fargo-area>
11. <https://www.theguardian.com/technology/2013/mar/28/damaged-undersea-cable-internet-disruption>
12. <http://gizmodo.com/5746121/how-egypt-turned-off-the-internet>
13. <http://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx>
14. http://www.theregister.co.uk/2012/08/29/saudi_aramco_malware_attack_analysis/
15. https://en.wikipedia.org/wiki/Denial-of-service_attack
16. https://en.wikipedia.org/wiki/Smart_city
17. DHS Software Assurance Marketplace (SWAMP); <https://continuousassurance.org/>